Cisco TelePresence SX20 Quick Set

ADMINISTRATOR GUIDE

- SX20 QUICK SET

Software version TC5.1
FEBRUARY 2012

Thank you for choosing Cisco!

Your Cisco product has been designed to give you many years of safe, reliable operation.

This part of the product documentation is aimed at administrators working with the setup of the MX200.

Our main objective with this Administrator guide is to address your goals and needs. Please let us know how well we succeeded!

May we recommend that you visit the Cisco web site regularly for updated versions of this guide.

The user documentation can be found on
- http://www.cisco.com/go/telepresence/docs.

How to use this guide

The top menu bar and the entries in the Table of contents are all hyperlinks. You can click on them to go to the topic.

Table of contents

Chapter 1

Introduction

This document provides you with the information required to administrate your product at an advanced level.

How to install the product and the initial configurations required are described in the Installation guide and Getting started guide, respectively.

Products covered in this guide

- Cisco TelePresence SX20 Quick Set

User documentation

The user documentation for the Cisco TelePresence systems running the TC software includes several guides suitable for various user groups.

- Video conference room primer
- Video conference room acoustics guidelines
- Installation guide
- Getting started guide for the Cisco TelePresence systems
- Software release notes for the TC software
- User guide for the TelePresence systems (with Touch controller)
- User guide for the TelePresence systems (with remote control)
- Quick reference guides for the TelePresence systems
- Administrator guide
- Regulatory compliance and safety information guide
- Legal & license information for products using TC software

Downloading the user documentation

We recommend you visit the Cisco web site regularly for updated versions of the user documentation.

Go to: ▸ http://www.cisco.com/go/telepresence/docs.

Guidelines how to find the documentation on the Cisco web site are included in the ▸ User documentation on the Cisco web site appendix.

Software

You can download the software for your product from the Cisco web site, go to:

▸ http://www.cisco.com/cisco/software/navigator.html

We recommend reading the Software Release Notes (TC5), go to:

▸ http://www.cisco.com/en/US/products/ps11424/tsd_products_support_series_home.html

Cisco contacts

On our web site you will find an overview of the worldwide Cisco contacts.

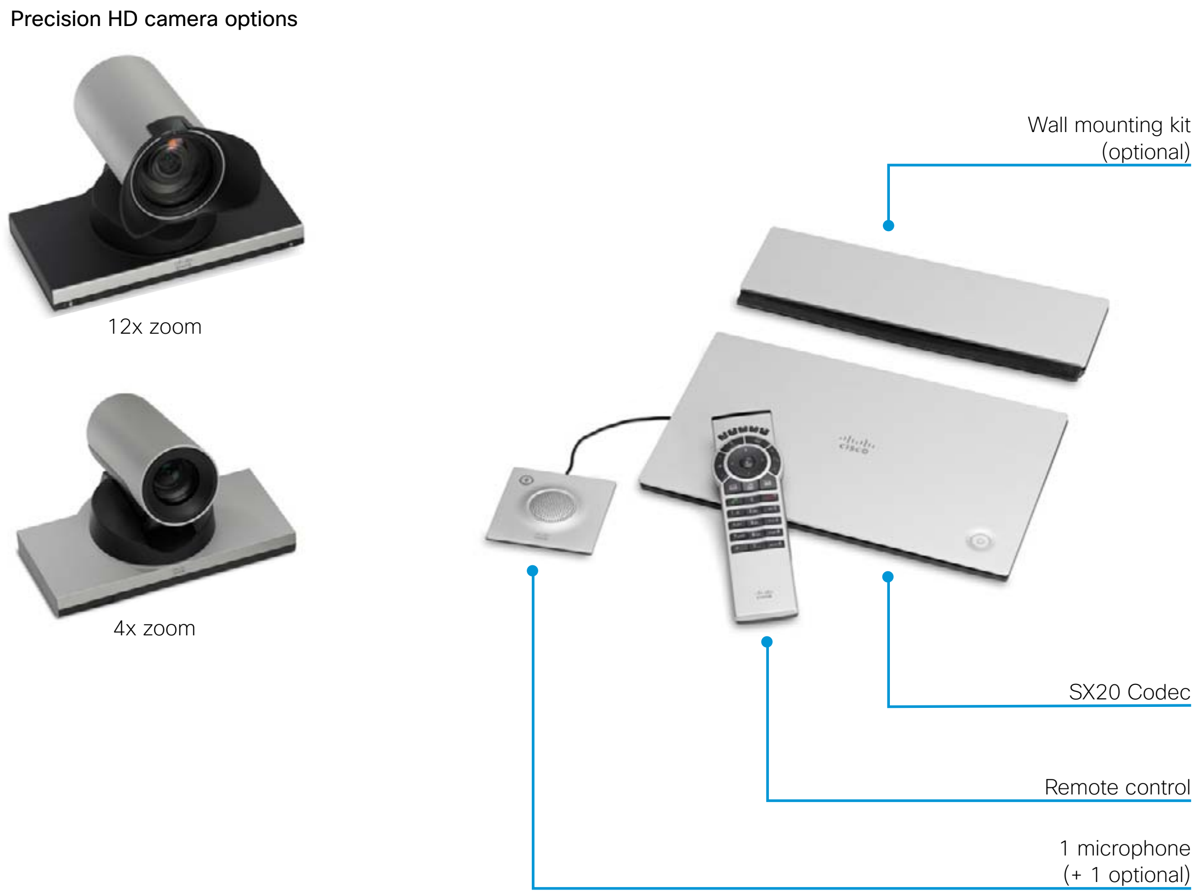
Go to: ▸ http://www.cisco.com/web/siteassets/contacts

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA

Cisco TelePresence SX20 Quick Set at a glance

The Cisco TelePresence® SX20 Quick Set can transform a standard flat panel display into a powerful telepresence system.

Whether you are just getting started with video communications or implementing a large-scale deployment, the SX20 Quick Set delivers high quality performance.


Precision HD camera options
12x zoom
4x zoom
Wall mounting kit (optional)
SX20 Codec
Remote control
1 microphone (+ 1 optional)

Features and benefits

- The system is easily installed. Also mounts easily on the wall (optional wall mount kit).
- The system is self-configuring with Cisco Unified Communications Manager (UCM) or Cisco Callway provisioning. All you need is to authenticate your endpoint to the network.
- Two PrecisionHD camera options with pan, tilt, and zoom helps ensure optimal framing and video clarity.
- Dedicated camera presets provide flexibility and easy viewing for any meeting scenario.
- Operation using remote controll and on-screen menu (default); or 8-inch Touch interface (optional).
- Simple *one-button-to-push* calling integrates with common calendar programs.
- Video resolution and frame rate up to 1080p60.
- You can connect and share your PC content at 1080p15 resolution and frame rate.
- Dual display option available.
- The systems support H.323 and Session Initiation Protocol (SIP) with bandwidth up to 6 Mbps point-to-point.
- The system is compatible with standards-based video systems without loss of features.
- Capabilities for multipoint conferences using the Cisco TelePresence Multiway™ technology, or the built in 4 way Cisco TelePresence MultiSite feature (no external bridge).

Chapter 2

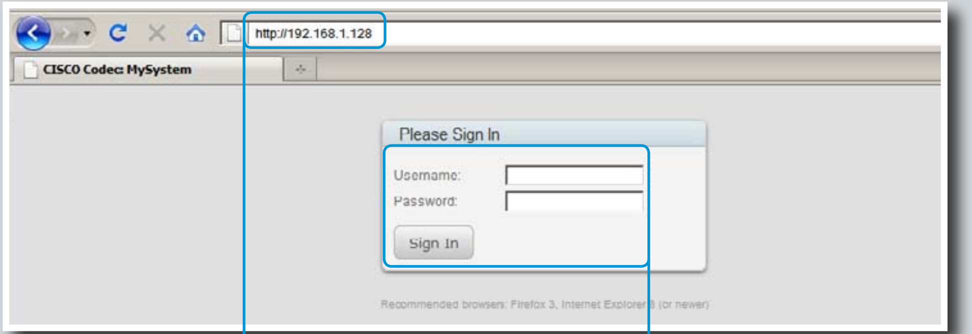
The web interface

Starting the web interface

The web interface provides full configuration access to your video conference system.

You can connect from a computer and administer the system remotely.

In the following you will find information how to use the web interface for system configuration and maintenance.



1. Connect to the video system

Open a web browser and enter the IP address of the video system in the address bar.

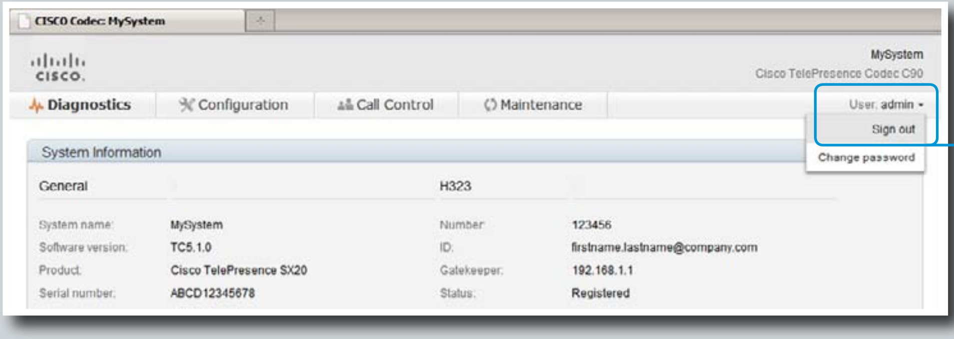
To find the IP address (IPv4 or IPv6), tap *More > Settings > System Information* on a Touch controller; or navigate to *Home > Settings > System information* when using a remote control and the on-screen menu.

2. Sign in

Enter the user name and password for your video system and press *Sign In*.

The system is delivered with a default user named **admin** with no password (i.e. leave the *Password* field blank when signing in for the first time).

NOTE: We strongly recommend that you set a password for the **admin** user to restrict access to system configuration, see the next page.



General		H323	
System name:	MySystem	Number:	123456
Software version:	TC5.1.0	ID:	firstname.lastname@company.com
Product:	Cisco TelePresence SX20	Gatekeeper:	192.168.1.1
Serial number:	ABCD12345678	Status:	Registered

Sign out

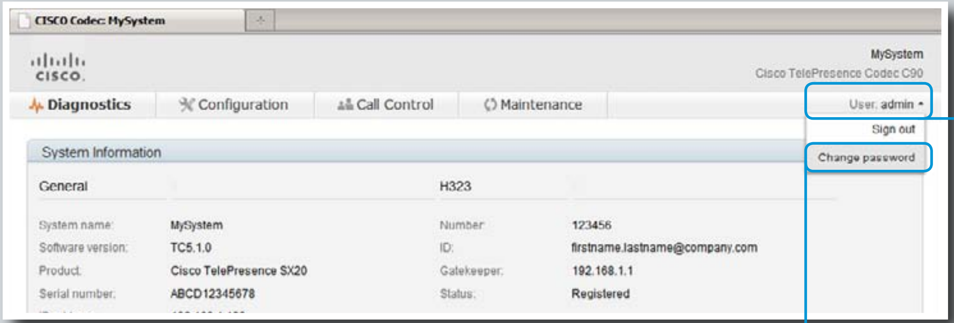
Click on your user name and select *Sign out* from the drop down menu.

Changing the system/codec password

You sign in to the web interface with the same user name and password as for the video conference system.

NOTE: We strongly recommend that you set a password for the default admin user, and any other users with ADMIN rights, to restrict access to system configuration.

You can read more about password protection in the ▸ Password protection appendices.



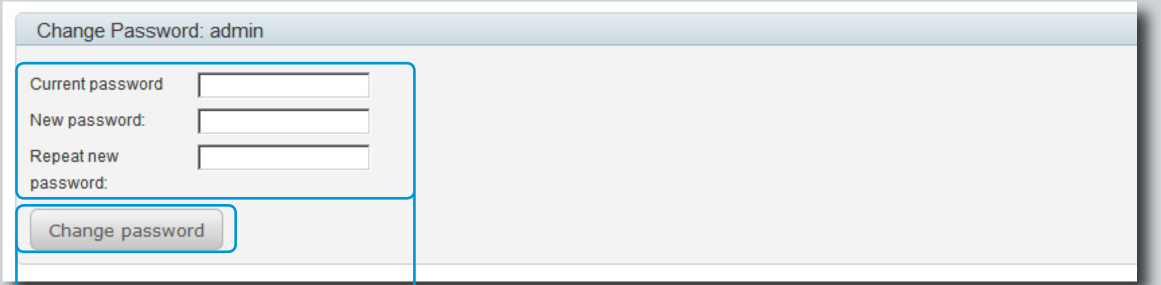
System Information

General		H323	
System name:	MySystem	Number:	123456
Software version:	TC5.1.0	ID:	firstname.lastname@company.com
Product:	Cisco TelePresence SX20	Gatekeeper:	192.168.1.1
Serial number:	ABCD12345678	Status:	Registered

1. Click your user name

2. Open the Change Password dialog box

Select *Change password* in the drop down menu.



Change Password: admin

Current password
New password:
Repeat new password:

3. Enter passwords

Enter your current and new passwords as requested. If the password currently is not set, leave the *Current password* field blank.

4. Set the new password

Press *Change password* for the change to take effect.

The interactive menu

The web interface provides access to tasks and configurations which are grouped in four categories. They are available from the main menu.

The main menu appears near the top of the page when you have signed in.

The sub-pages for the different tasks are described on the following pages.

Menu availability and user roles

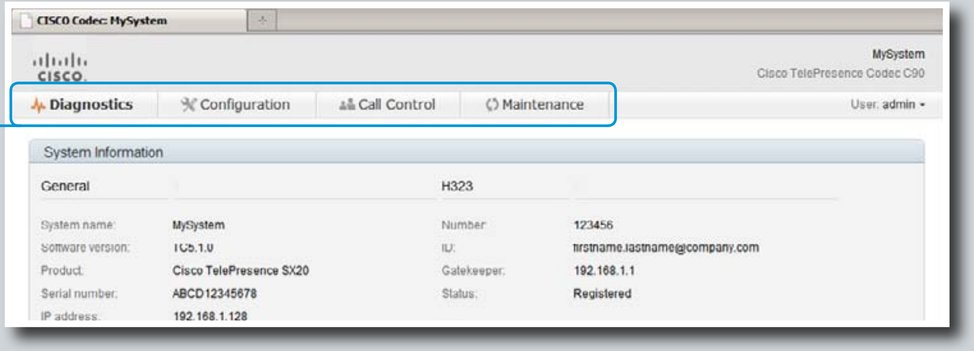
A user possesses one or more user roles. Three user roles are defined: ADMIN, AUDIT and USER. Note that the default admin user holds all three roles. [1]

The table below shows which menus are available for users holding the different roles.

	ADMIN	AUDIT	USER
Diagnostics			
System Information	✓	✓	✓
Log Files	✓		
XML Files	✓		
Configuration			
Advanced Configuration	✓	✓	
Wallpaper	✓		
Sign In Banner	✓		
Call Control			✓
Maintenance			
Software Upgrade	✓		
Certificate Management	✓		
Audit Certificate		✓	
User Administration	✓		
Restart			✓
Factory Reset	✓		

Main menu

- Diagnostics
- Configuration
- Call Control
- Maintenance



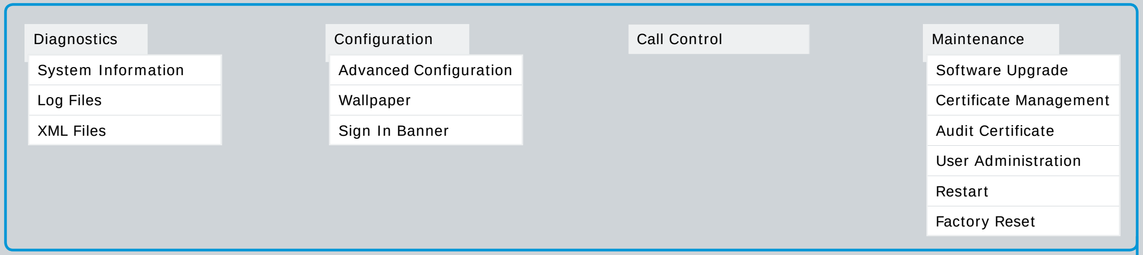
System Information

General

System name: MySystem
Software version: TC5.1.0
Product: Cisco TelePresence SX20
Serial number: ABCD12345678
IP address: 192.168.1.128

H323

Number: 123456
ID: firstname.lastname@company.com
Gatekeeper: 192.168.1.1
Status: Registered



Diagnostics
- System Information
- Log Files
- XML Files

Configuration
- Advanced Configuration
- Wallpaper
- Sign In Banner

Call Control

Maintenance
- Software Upgrade
- Certificate Management
- Audit Certificate
- User Administration
- Restart
- Factory Reset

Open sub-pages

When you hover the mouse over a main menu item, the titles of related sub-pages appear. [2]

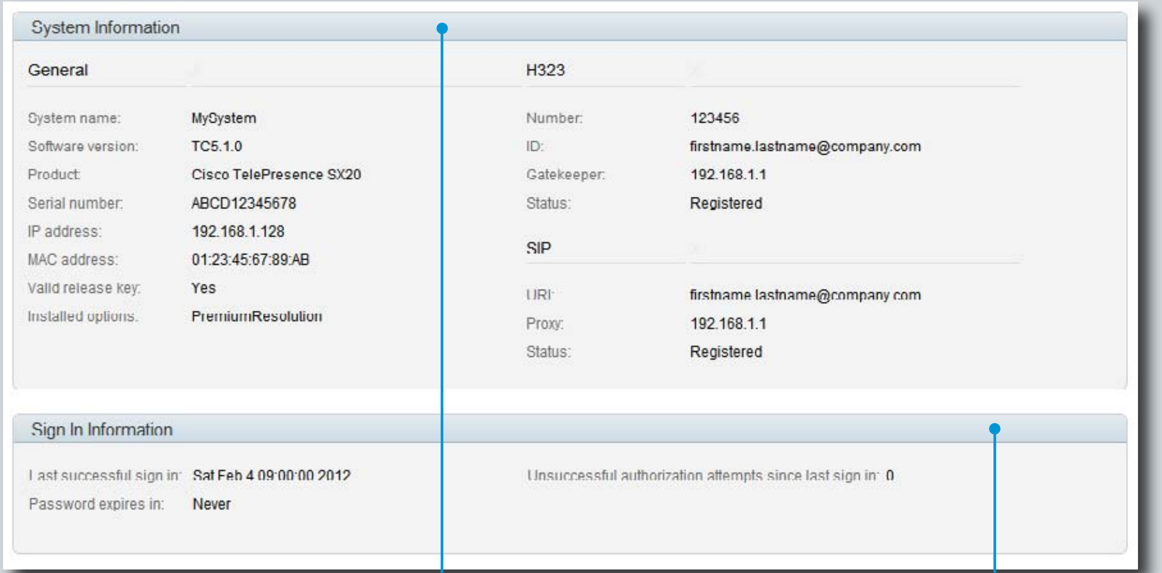
Click a sub-page's title to open it. If there are no related sub-pages, click the main menu item itself.

[1] You can read more about user administration and user roles in the ▸ User administration section.

[2] The illustration lists all the sub-menus. A user not possessing all user roles will only see the sub-set relevant for his type of user.

The system information page

You can find an overview of your video system set-up on the System Information page.



System Information

General

System name:	MySystem
Software version:	TC5.1.0
Product:	Cisco TelePresence SX20
Serial number:	ABCD12345678
IP address:	192.168.1.128
MAC address:	01:23:45:67:89:AB
Valid release key:	Yes
Installed options:	PremiumResolution

H323

Number:	123456
ID:	firstname.lastname@company.com
Gatekeeper:	192.168.1.1
Status:	Registered

SIP

URI:	firstname.lastname@company.com
Proxy:	192.168.1.1
Status:	Registered

Sign In Information

Last successful sign in:	Sat Feb 4 09:00:00 2012
Password expires in:	Never

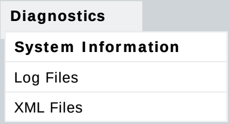
Unsuccessful authorization attempts since last sign in: 0

System information

Information about system name, product type, software version, IP address, etc.

Login information

Information about recent login attempts and password expiry.



Log files

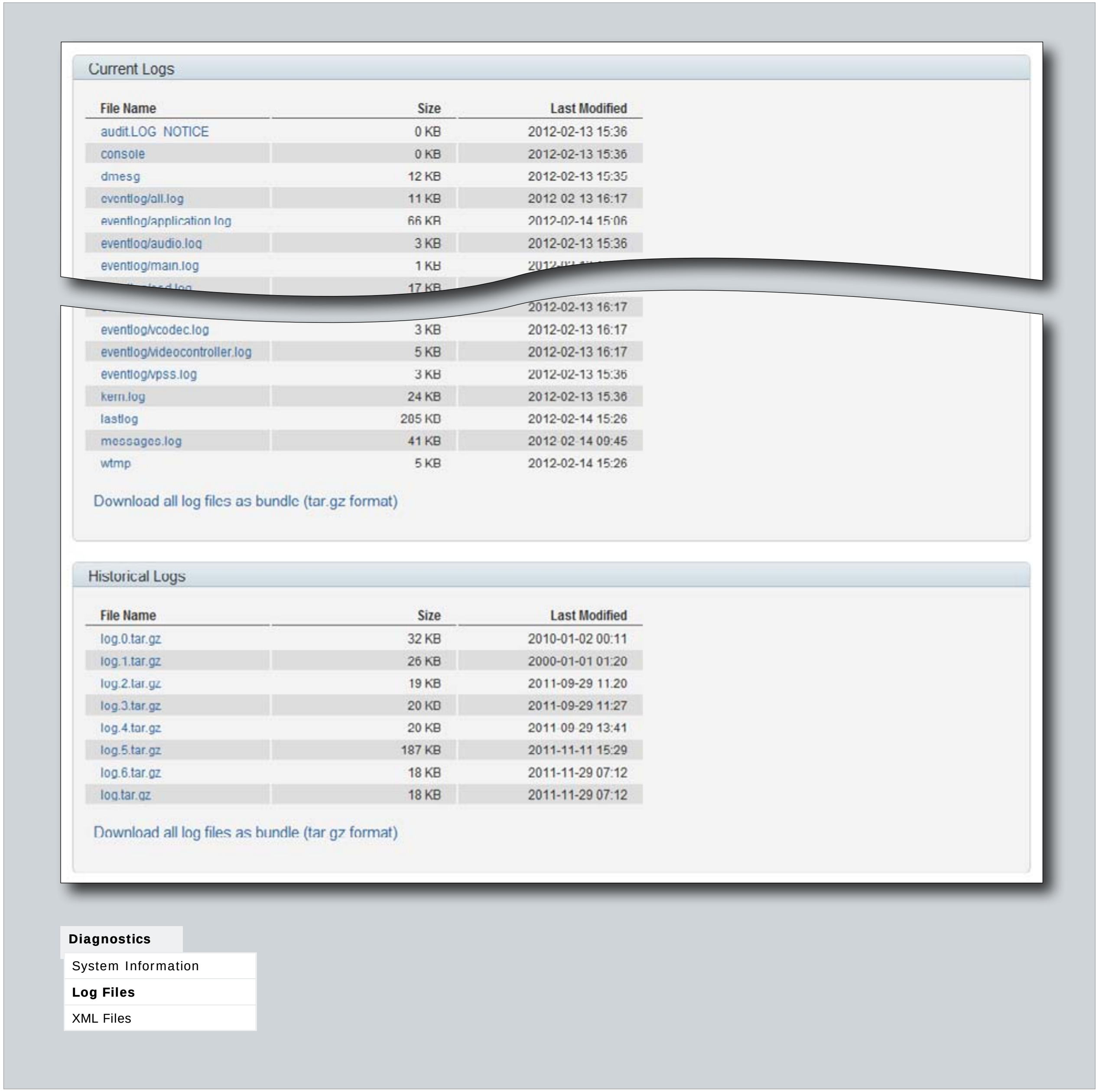
The log files are Cisco specific debug files which may be requested by the Cisco support organization if you need technical support.

The current log files are time stamped event log files.

All current log files are archived in a time stamped historical log file each time the system reboots.

Click on a log file and follow the instructions in the dialog box to save or open the file (left or right click depending on your browser).

You can also download all log files as a bundle; click the corresponding link on the web page and follow the instructions.



Current Logs

File Name	Size	Last Modified
audit.LOG_NOTICE	0 KB	2012-02-13 15:36
console	0 KB	2012-02-13 15:36
dmesg	12 KB	2012-02-13 15:35
eventlog/all.log	11 KB	2012 02 13 16:17
eventlog/application log	66 KB	2012-02-14 15:06
eventlog/audio.log	3 KB	2012-02-13 15:36
eventlog/main.log	1 KB	[illegible]
[illegible]	17 KB	[illegible]
		2012-02-13 16:17
eventlog/vcodec.log	3 KB	2012-02-13 16:17
eventlog/videocontroller.log	5 KB	2012-02-13 16:17
eventlog/vpss.log	3 KB	2012-02-13 15:36
kern.log	24 KB	2012-02-13 15:36
lastlog	205 KB	2012-02-14 15:26
messages.log	41 KB	2012 02 14 09:45
wtmp	5 KB	2012-02-14 15:26

Download all log files as bundle (tar.gz format)

Historical Logs

File Name	Size	Last Modified
log.0.tar.gz	32 KB	2010-01-02 00:11
log.1.tar.gz	26 KB	2000-01-01 01:20
log.2.tar.gz	19 KB	2011-09-29 11:20
log.3.tar.gz	20 KB	2011-09-29 11:27
log.4.tar.gz	20 KB	2011 09 29 13:41
log.5.tar.gz	187 KB	2011-11-11 15:29
log.6.tar.gz	18 KB	2011-11-29 07:12
log.tar.gz	18 KB	2011-11-29 07:12

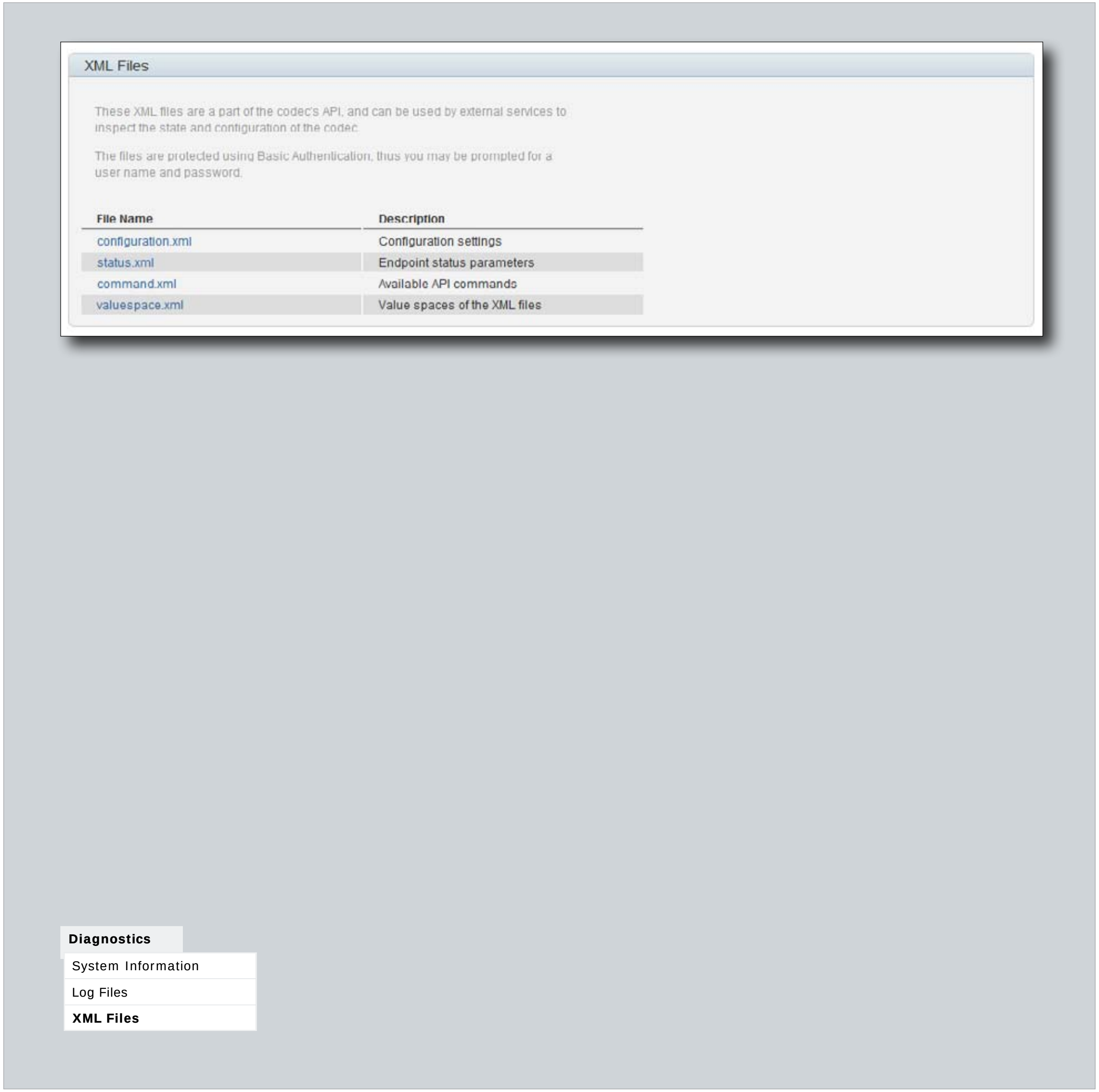
Download all log files as bundle (tar gz format)

XML files

The XML files are structured in a hierarchy building up a database of information about the codec.

Click the file names to open the corresponding file.

- Select *configuration.xml* to see an overview of the system settings, which are controlled from the web interface or from the API (Application Programmer Interface).
- The information in *status.xml* is constantly updated by the system to reflect system and process changes. The status information is normally monitored from the API.
- Select *command.xml* to see an overview of the commands available to instruct the system to perform an action. The commands are issued from the API.
- Select *valuespace.xml* to see an overview of all the value spaces used in the system settings, status information, and commands.



XML Files

These XML files are a part of the codec's API, and can be used by external services to inspect the state and configuration of the codec.

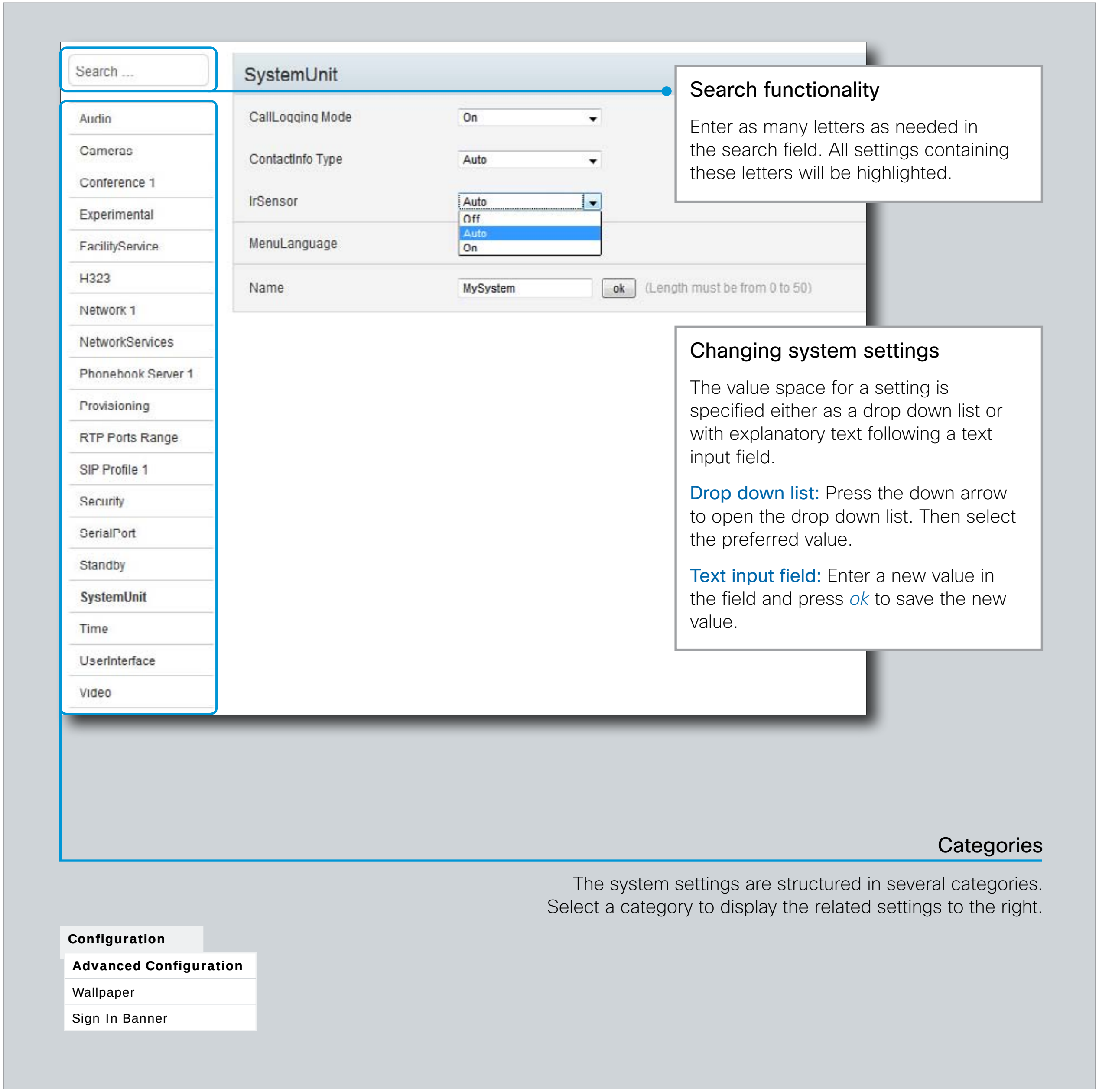
The files are protected using Basic Authentication, thus you may be prompted for a user name and password.

File Name	Description
configuration.xml	Configuration settings
status.xml	Endpoint status parameters
command.xml	Available API commands
valuespace.xml	Value spaces of the XML files

Advanced configuration

The system settings are grouped in several categories. When you select a category in the left column, all related settings appear in the window to the right.

Each system setting is further described in the ▸ Advanced settings chapter.



SystemUnit

CallLogging Mode: On

ContactInfo Type: Auto

IrSensor: Auto (Off / Auto / On)

MenuLanguage

Name: MySystem ok (Length must be from 0 to 50)

Search functionality

Enter as many letters as needed in the search field. All settings containing these letters will be highlighted.

Changing system settings

The value space for a setting is specified either as a drop down list or with explanatory text following a text input field.

Drop down list: Press the down arrow to open the drop down list. Then select the preferred value.

Text input field: Enter a new value in the field and press *ok* to save the new value.

Categories

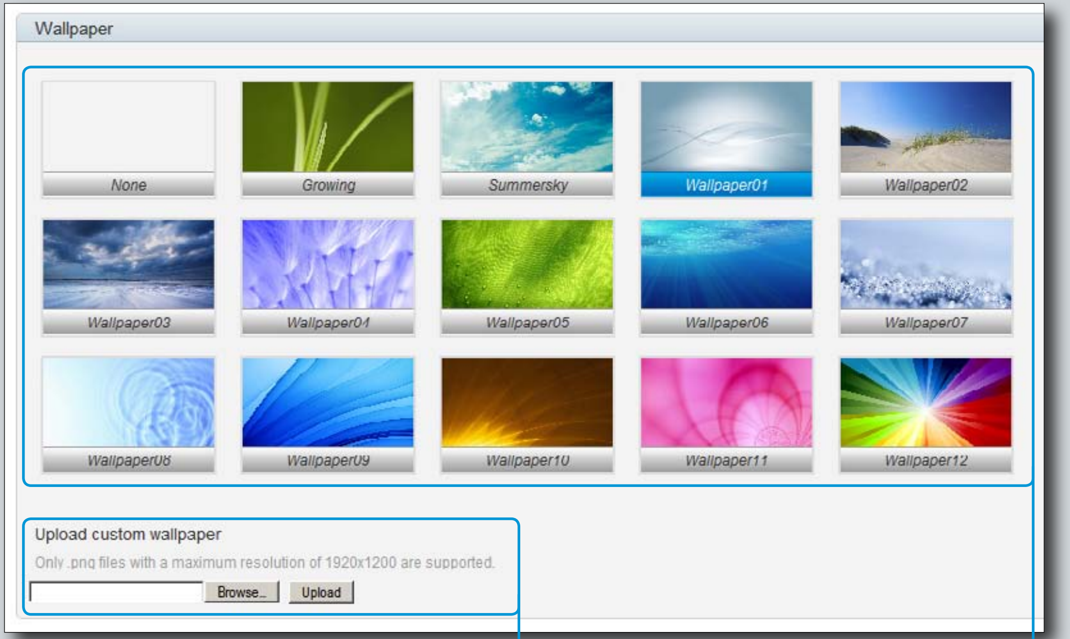
The system settings are structured in several categories. Select a category to display the related settings to the right.

Selecting a wallpaper

You can select between a set of predefined wallpapers as background on your display.

If you want the company logo or another custom picture to be displayed on the main display, you may also upload and use a custom wallpaper.

If you use the Touch controller: The custom wallpaper applies to the main display only and will not appear on the Touch controller.



Only .png files with a maximum resolution of 1920x1200 are supported.

Upload a custom wallpaper file

i. Press *Browse...* and locate your custom wallpaper image file.

The file format must be .png and the maximum image size is 1920 × 1200 pixels.

ii. Press *Upload* to save the file to the codec.

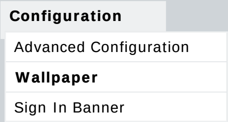
The custom wallpaper is selected automatically upon upload.

Select a wallpaper

Select a wallpaper from the list.

If you have uploaded a custom wallpaper, it will also appear in the list.

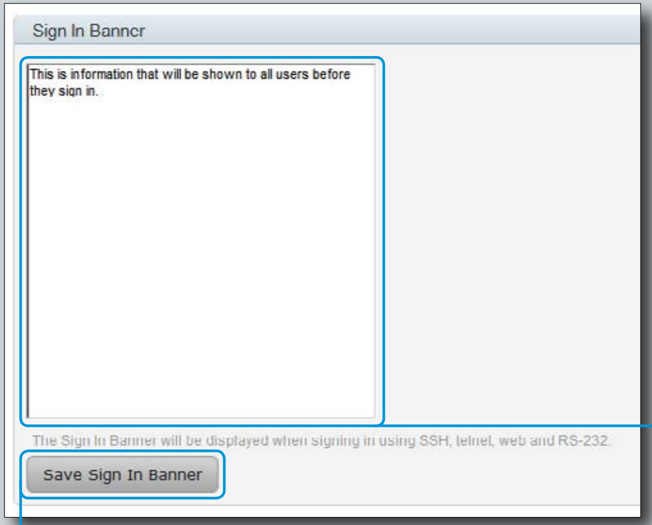
The selected wallpaper is highlighted.



Sign in banner

If a system administrator wants to provide initial information to all users, he can create a sign in banner. A sign in banner is a message that is displayed to the user before signing in.

The message will be shown when the user signs in to the web interface or the command line interface.



Sign In Banner

This is information that will be shown to all users before they sign in.

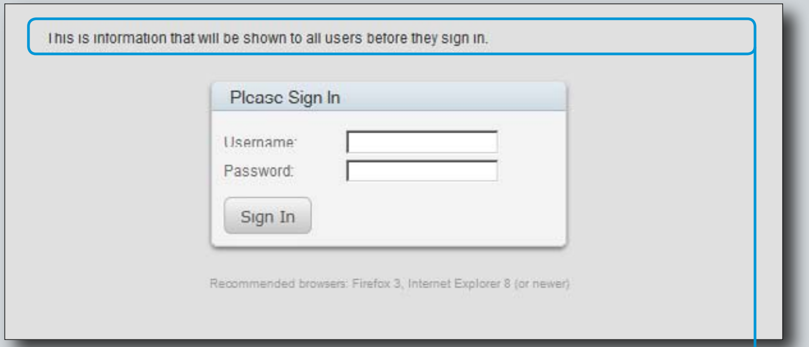
The Sign In Banner will be displayed when signing in using SSH, telnet, web and RS-232.

1. Enter text for the sign in banner

Enter the text message which you want to present to the user prior to signing in.

2. Activate the sign in banner

Press *Save Sign In Banner* to activate it.

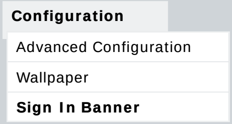


This is information that will be shown to all users before they sign in.

Recommended browsers: Firefox 3, Internet Explorer 8 (or newer)

An active sign in banner

The sign in banner is displayed here.



Placing a call

You can use the Call Control page of the web interface to initiate a call.

NOTE: Even if the web interface is used to initiate the call it is the video system (display, microphones and loudspeakers) that is used for the call; not the PC running the web interface.

Calling someone

Enter one or more characters in the address input field until the name you want to call appears in the dynamic search list or, enter the complete name or number. Then press *Dial*.

Press *End all* to disconnect the call.

Calling more than one

A point-to-point video call (a call involving two parties only) may be expanded to include more participants if your system supports the optional built-in MultiSite feature (up to four participants, yourself included). The call will then become a video conference.

When in a call, enter the name or number of the next participant in the address input field, and then press *Dial*.

Press *End all* to terminate the entire conference.

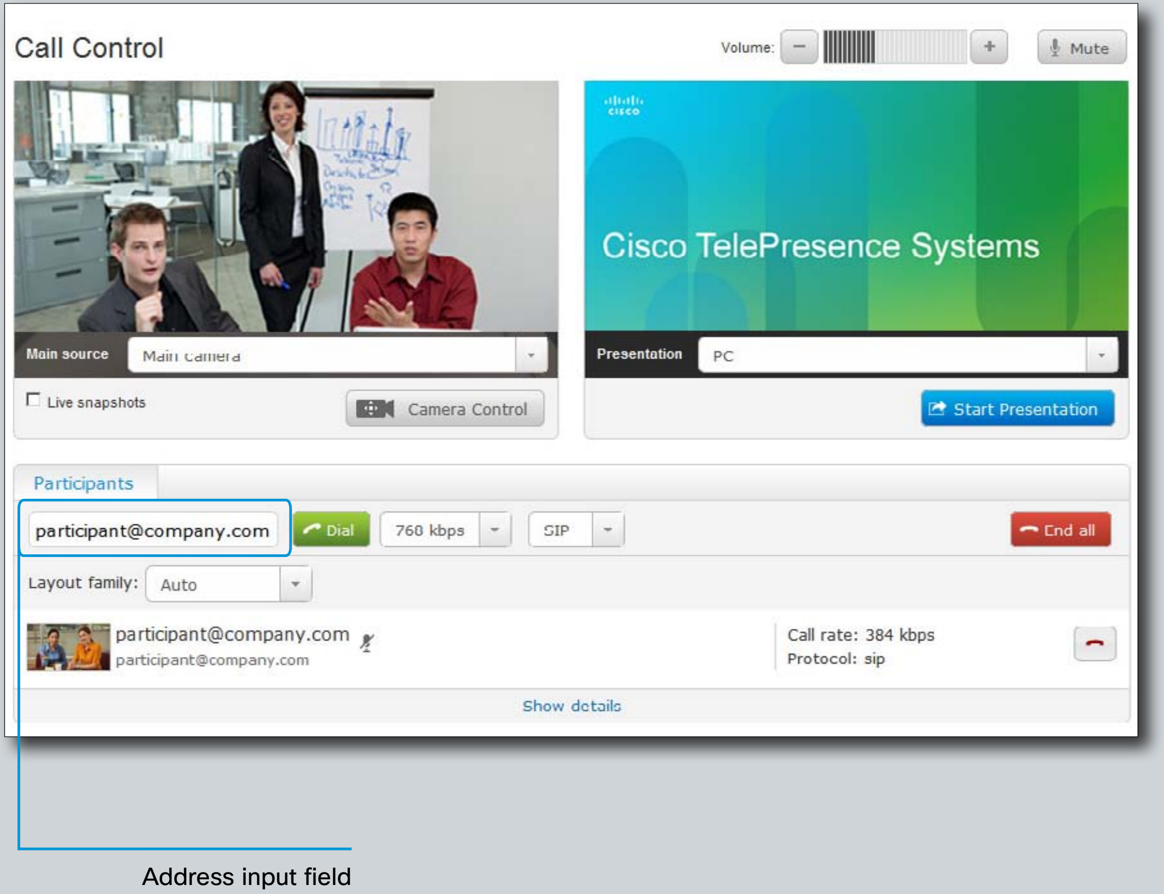
To disconnect just one of the participants, press the ☎ button for that participant.

Sharing contents

Select a Presentation Source from the drop down list, and press the *Start Presentation* button.

Normally a PC is used as presentation source, but other options may be available depending on your system setup.

To stop the content sharing, press the *Stop Presentation* button that becomes visible while sharing.



Call Control

Volume: − +

Main source: Main camera

☐ Live snapshots

Presentation: PC

Participants

participant@company.com — 768 kbps — SIP

Layout family: Auto

participant@company.com
participant@company.com

Call rate: 384 kbps
Protocol: sip

Call Control

Controlling and monitoring a call

You can control and monitor several call features using the Call Control page.

Adjusting the sound volume

Use + and - on the volume control bar to adjust the sound volume of your system (not the keyboard + and - keys).

Muting the microphone

Use the *Mute* button when you want to deactivate the microphone for privacy reasons.

When the microphone is muted, the button is replaced by an *Unmute* button. Use this button to re-activate the microphone.

Controlling the camera

First, press the *Camera Control* button. Then, in the window that opens, use + and - to adjust the zoom and the arrow keys to adjust the camera's angle.

If a camera preset is defined it is listed to the right. Apply the preset by clicking its name.

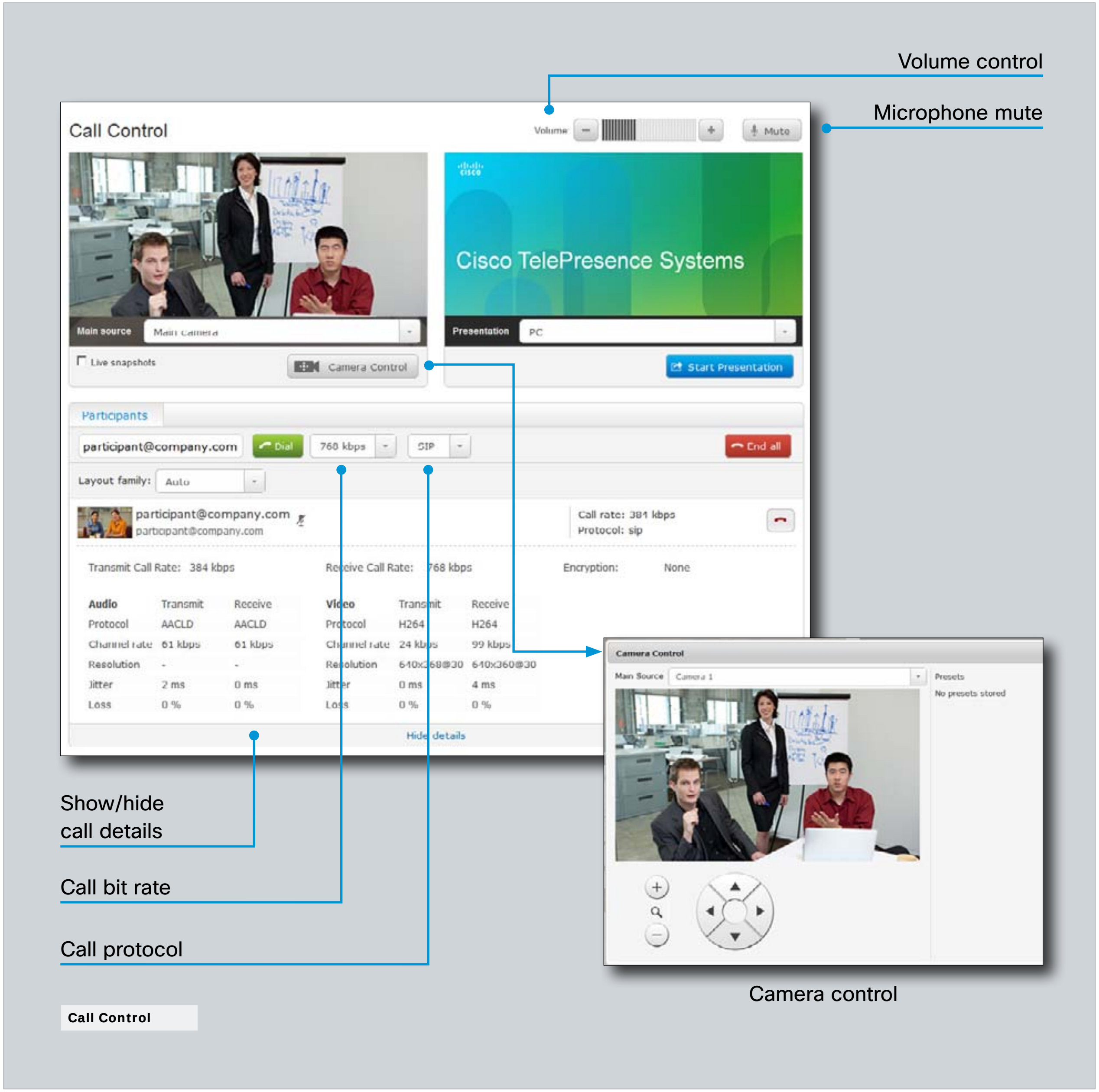
Call settings

When you load the Call Control page, the default call bit rate and the default call protocol are shown in the *Call bit rate* and *Call protocol* fields, respectively. If preferred, you can select another bit rate or another protocol from the drop down lists. You can not change these settings during a call.

Call details

Press *Show details* while in a call to provide information on call rate, encryption, as well as important video and audio parameters.

Hide details removes the information.



Call Control

Main source: Main camera
Presentation: PC
□ Live snapshots

participant@company.com | 768 kbps | SIP

Layout family: Auto

participant@company.com
participant@company.com

Call rate: 384 kbps
Protocol: sip

Transmit Call Rate: 384 kbps | Receive Call Rate: 768 kbps | Encryption: None

Audio	Transmit	Receive	Video	Transmit	Receive
Protocol	AACLD	AACLD	Protocol	H264	H264
Channel rate	61 kbps	61 kbps	Channel rate	24 kbps	99 kbps
Resolution	-	-	Resolution	640x368@30	640x360@30
Jitter	2 ms	0 ms	Jitter	0 ms	4 ms
Loss	0 %	0 %	Loss	0 %	0 %

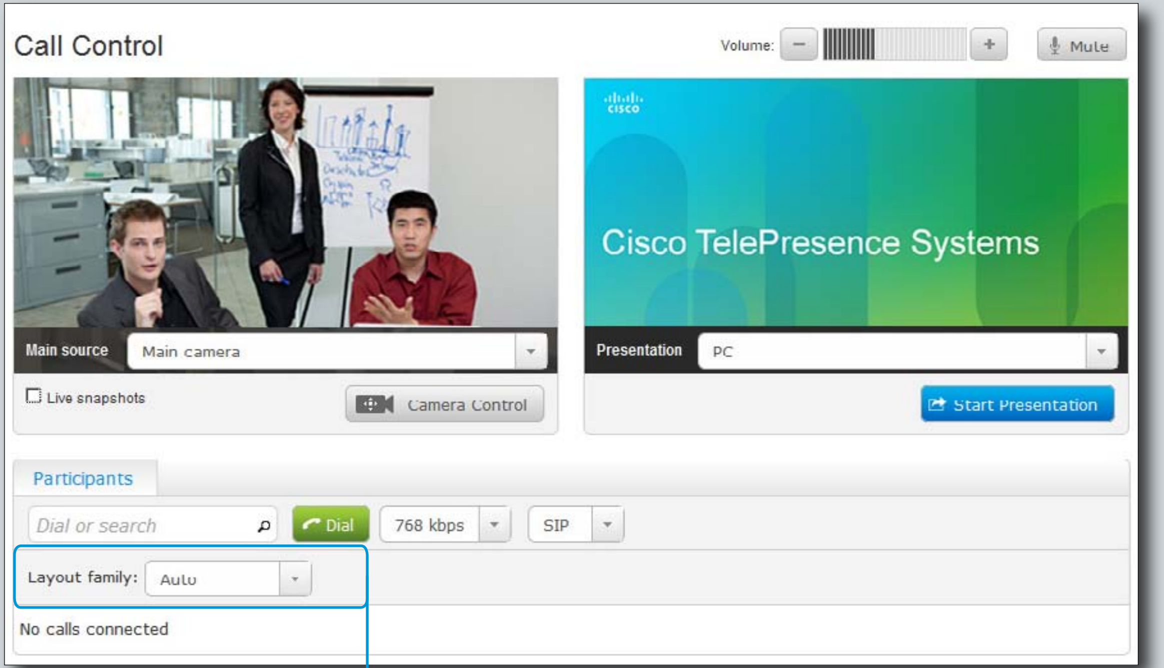
Camera Control
Main Source: Camera 1
Presets
No presets stored

Local layout control

You can select a local layout using the Call Control page.

The term layout is used to describe the various ways a video conversation appear on screen. Different types of meetings will require different layouts.

Each layout will typically specify a screen layout well suited when you are not in a meeting or you are in a meeting with one, two or three parties; when the meeting does or does not involve a second video stream for presentations; when the screen aspect ratio is 4:3 or 16:9.


Call Control

Main source: Main camera

Presentation: PC

☐ Live snapshots

Dial or search

768 kbps

SIP

Layout family: Auto

No calls connected

Select a layout

Select your preferred layout in the drop down menu. You may change the layout while in a call.

Call Control

Capturing snapshots

The snapshot feature, which is disabled by default, allows snapshots captured by your video system to be displayed on the Call Control page. Captures from your video system's camera as well as from its presentation channel will by displayed.

This feature might come in handy when administering the video system from a remote location, e.g. to check the camera view.

To use web snapshots you have to sign in with ADMIN credentials.

Enabling the snapshot feature

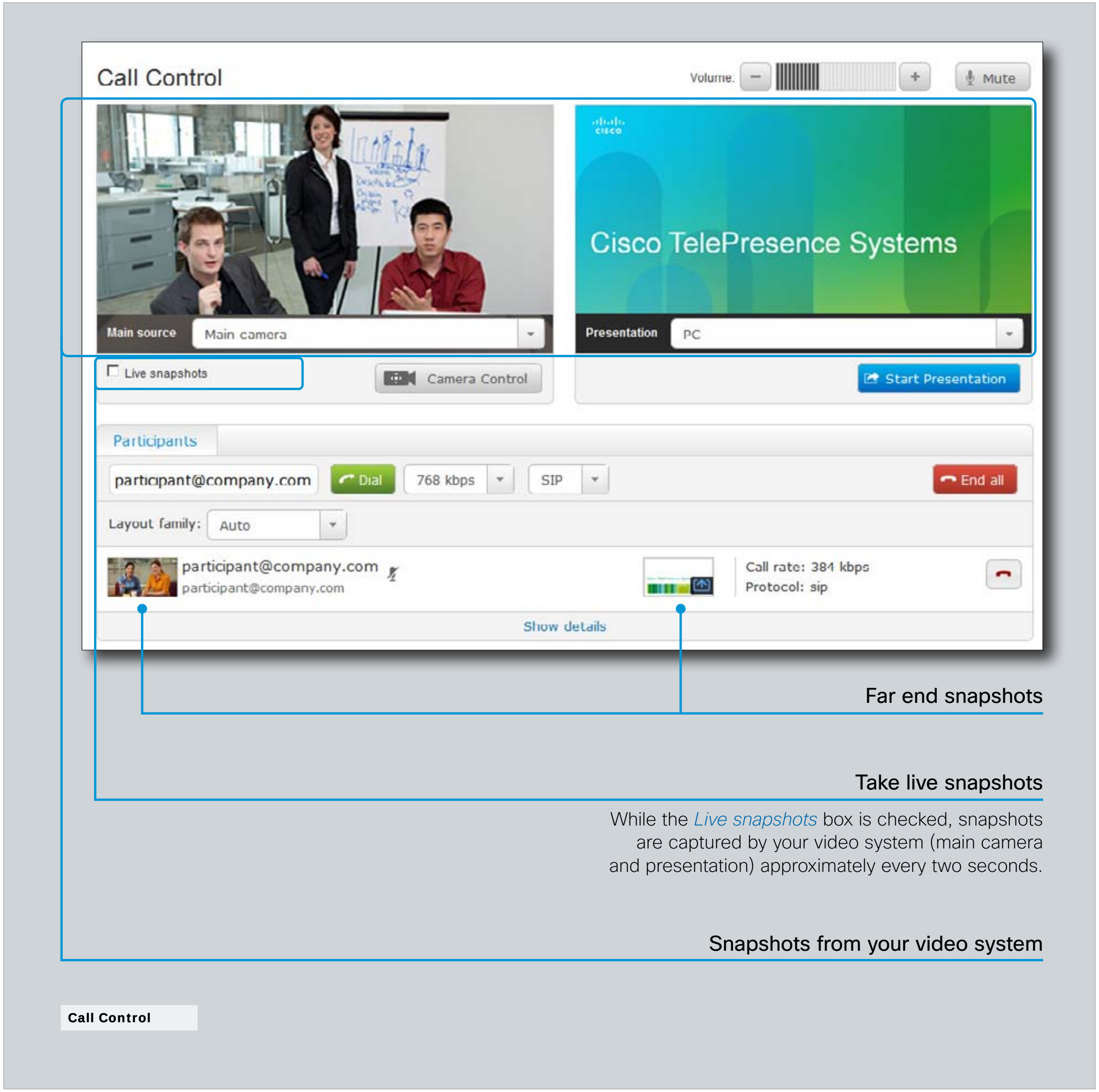
The snapshot feature is disabled by default, and must be enabled using the Touch controller or the remote control and on screen menu.

- Touch controller: Tap *More > Settings > Administrator Settings > Web Snapshots* and select On.
- Remote control and on screen menu: Go to the Advanced configuration menu, navigate to *Video > AllowWebSnapshots* and select On.

Far end snapshots while in a call

While in a call, snapshots of the remote participant's main camera and presentation channel (far end) will be captured and displayed as shown in the illustration. The snapshots are updated approximately every 20 seconds.

NOTE: Far end snapshots are captured even if web snapshots are disallowed on the far end video system. Web snapshots are prohibited only for encrypted calls.



Main source: Main camera

Presentation: PC

□ Live snapshots

participant@company.com | 768 kbps | SIP

Layout family: Auto

participant@company.com
participant@company.com

Call rate: 384 kbps
Protocol: sip

Far end snapshots

Take live snapshots

While the *Live snapshots* box is checked, snapshots are captured by your video system (main camera and presentation) approximately every two seconds.

Snapshots from your video system

Call Control

Upgrading the system software

From the Upgrade Software page you can initiate software upgrades and add a release key and option keys.

Software versions

This video conference system is using TC software.

NOTE: Contact your system administrator if you have questions about the software version.

Software release notes and upgrade files

For a complete overview of the news and changes, we recommend reading the Software Release Notes (TC5).

Go to: ▸ http://www.cisco.com/en/US/products/ps11424/tsd_products_support_series_home.html

Downloading new software

For software download, go to: ▸ http://www.cisco.com/cisco/software/navigator.html

Release key

The release key is required to be able to use the released software. A new release key is required for every major software release (e.g. from TC4.x to TC5.x).

Contact your Cisco representative to obtain the release key.

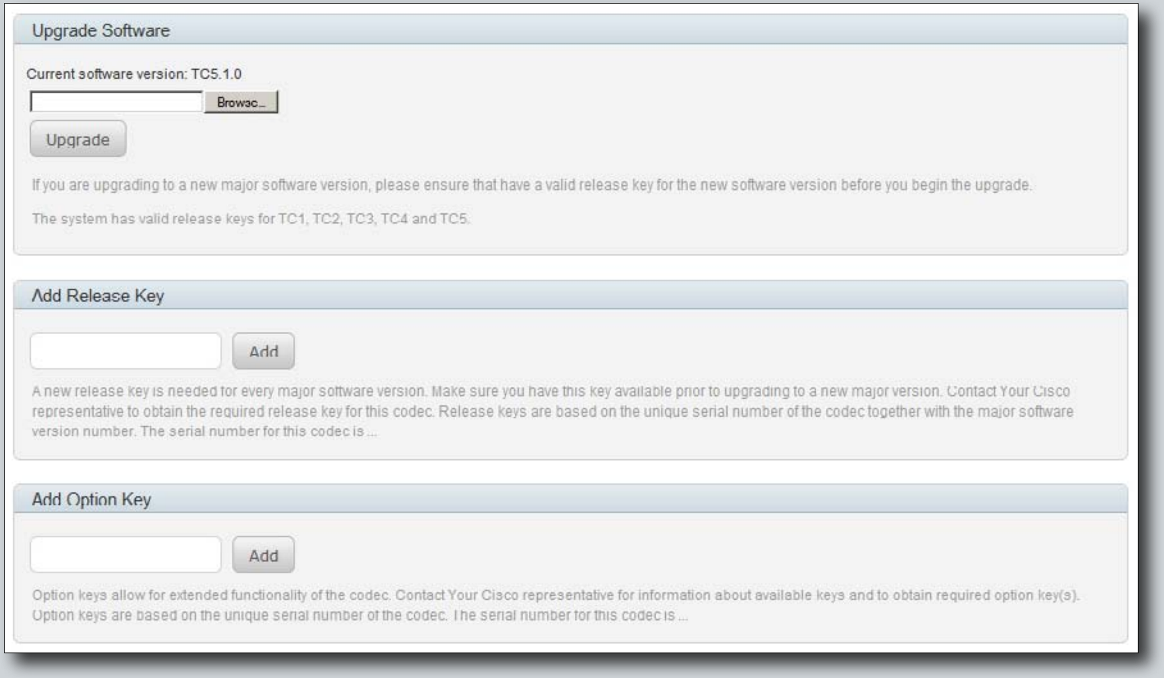
Option keys

Option keys allow for extended functionality of the system. The keys are required to activate the optional functionality. You may have several option keys in your system.

The available options are:

- Premium resolution
- MultiSite
- Dual display

Contact your Cisco representative to obtain the option keys.



Upgrade Software

Current software version: TC5.1.0

If you are upgrading to a new major software version, please ensure that have a valid release key for the new software version before you begin the upgrade.

The system has valid release keys for TC1, TC2, TC3, TC4 and TC5.

Add Release Key

A new release key is needed for every major software version. Make sure you have this key available prior to upgrading to a new major version. Contact Your Cisco representative to obtain the required release key for this codec. Release keys are based on the unique serial number of the codec together with the major software version number. The serial number for this codec is ...

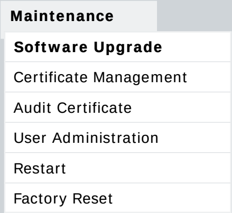
Add Option Key

Option keys allow for extended functionality of the codec. Contact Your Cisco representative for information about available keys and to obtain required option key(s). Option keys are based on the unique serial number of the codec. The serial number for this codec is ...

1. Add the release and option keys

Contact your Cisco representative to obtain the required key(s). To add a release key and one or more option keys, complete the following steps:

i. Enter the *Release Key* and press *Add*. Key format: “1TC005-1-0C22E348” (each system has a unique key).



ii. Enter the *Option Key* and press *Add*. Key format: “1N000-1-AA7A4A09” (each system has a unique key).

iii. If you have more than one option key, repeat step ii for all of them.

2. Upgrade the software on the codec

i. Before you can start the upgrade you must download the software upgrade file. The file format is “s52010tc5_1_0.pkg” (each software version has a unique file name).

ii. Press *Browse...* and select the .PKG file.

iii. Press *Upgrade* to start the installation.

iv. Allow the installation process to complete. It may take up to 30 minutes. You can follow the progress on the web page.

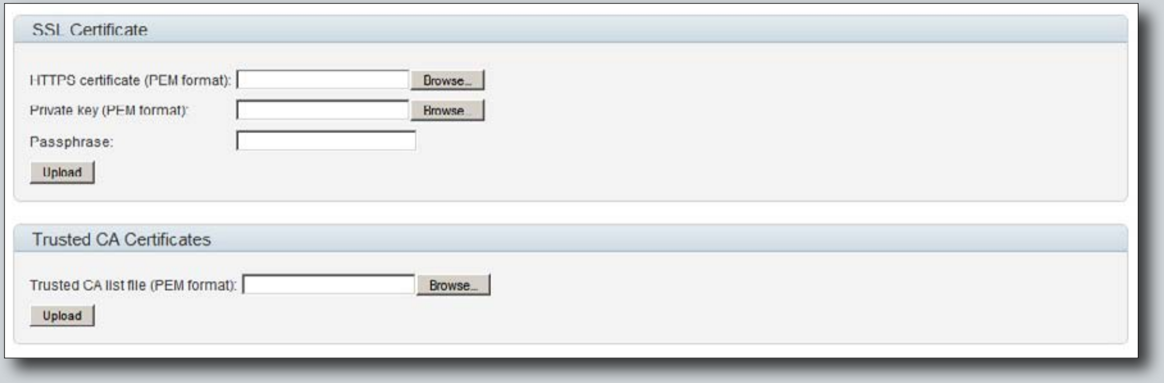
The system reboots automatically after the installation, and the connection to the web interface is lost.

If you want to continue working with the web interface you must re-establish the connection and sign in anew.

Certificate management

The SSL certificate is a text file which verifies the authenticity of your video conference system. The certificate may be issued by a certificate authority (CA). Other parties can check this certificate before setting up communication with you.

The list of trusted CA certificates is a list containing the SSL certificates of all parties that you want your system to trust.



SSL Certificate

HTTPS certificate (PEM format): Browse...
Private key (PEM format): Browse
Passphrase:
Upload

Trusted CA Certificates

Trusted CA list file (PEM format): Browse...
Upload

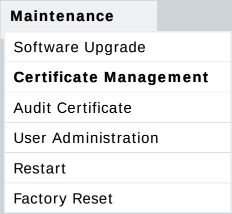
Uploading the trusted CA certificates list

To install the trusted CA certificates list, you will need the following:

- Trusted CA list file (.PEM format).

Contact your system administrator to obtain the required file.

1. Press *Browse...* and locate the file with the Trusted CA list (.PEM format).
2. Press *Upload* to store the certificate list on your system.



Uploading the SSL certificate

To install the SSL certificate, you will need the following:

- HTTPS certificate (.PEM format)
- Private key (.PEM format)
- Passphrase (optional)

Contact your system administrator to obtain the required files.

1. Press *Browse...* and locate the HTTPS certificate file (.PEM format).
2. Press *Browse...* and locate the Private key file (.PEM format).
3. Enter the *Passphrase*.
4. Press *Upload* to store the certificate on your system.

The audit certificate list

If you want to use the ExternalSecure audit logging mode, you must upload a list of trusted audit certificates to the video conference system. This list must cover all audit servers that your system shall trust.

In the ExternalSecure audit logging mode audit logging information will only be sent to entities holding a valid audit certificate.

NOTE: You must always upload the audit certificate list before enabling secure audit logging.

About audit logging

Audit logging records all sign in activity and configuration changes on the system.

Audit logging is disabled by default. You can enable audit logging using the on-screen menu or the web interface.

1. Upload the audit certificate list

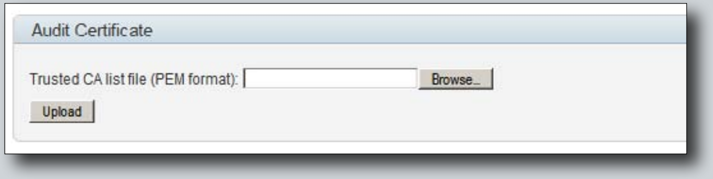
To install the audit certificate, you will need:

- Audit list file (.PEM format)

Contact your system administrator to obtain the required file.

i. Press *Browse...* and locate the file with the audit list file (.PEM format).

ii. Press *Upload* to store the certificate on your system.



Audit Certificate

Trusted CA list file (PEM format):

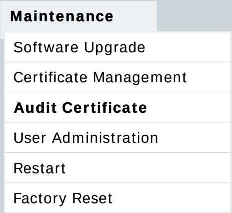
2. Enable secure audit logging

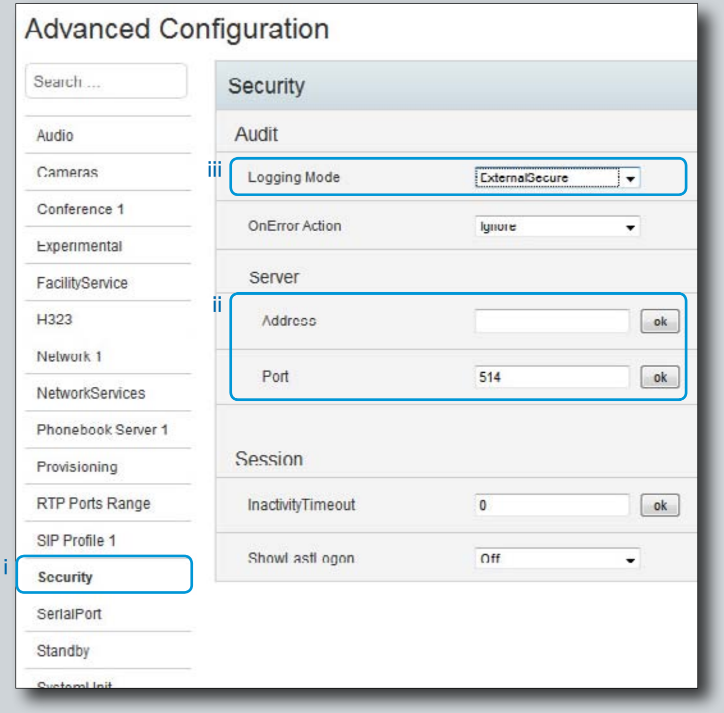
When you have uploaded the audit certificate list you must enable secure audit logging:

i. Select *Advanced Configuration* under the *Configuration* tab. Then select *Security* in the list of settings groups on the left hand side.

ii. Enter the *Address* and *Port* number of the audit server.

iii. Select ExternalSecure from the *Logging Mode* drop down list.





Advanced Configuration

Security

Audit

Logging Mode: ExternalSecure

OnError Action: Ignore

Server

Address:

Port: 514

Session

InactivityTimeout: 0

Showl astl ogon: Off

User administration

From this page you can manage the user accounts of your video conference system. You can create new user accounts, edit the details of existing users, and delete users.

The default user account

The system comes with a default administrator user account with username admin and no password set. The admin user has full access rights, and it is highly recommended to set a password for this user.

Read more about passwords in the ▸ Password protection appendices.

About user roles

A user account must hold one or a combination of several user roles. Three user roles exist, representing different rights:

- ADMIN: A user holding this role can create new users and change all settings, except the security audit settings. He cannot upload audit certificates.
- USER: A user holding this role can make calls and search the phonebook.
- AUDIT: A user holding this role can change the security audit configurations and upload audit certificates.

It is important to note that these three roles have non-overlapping rights.

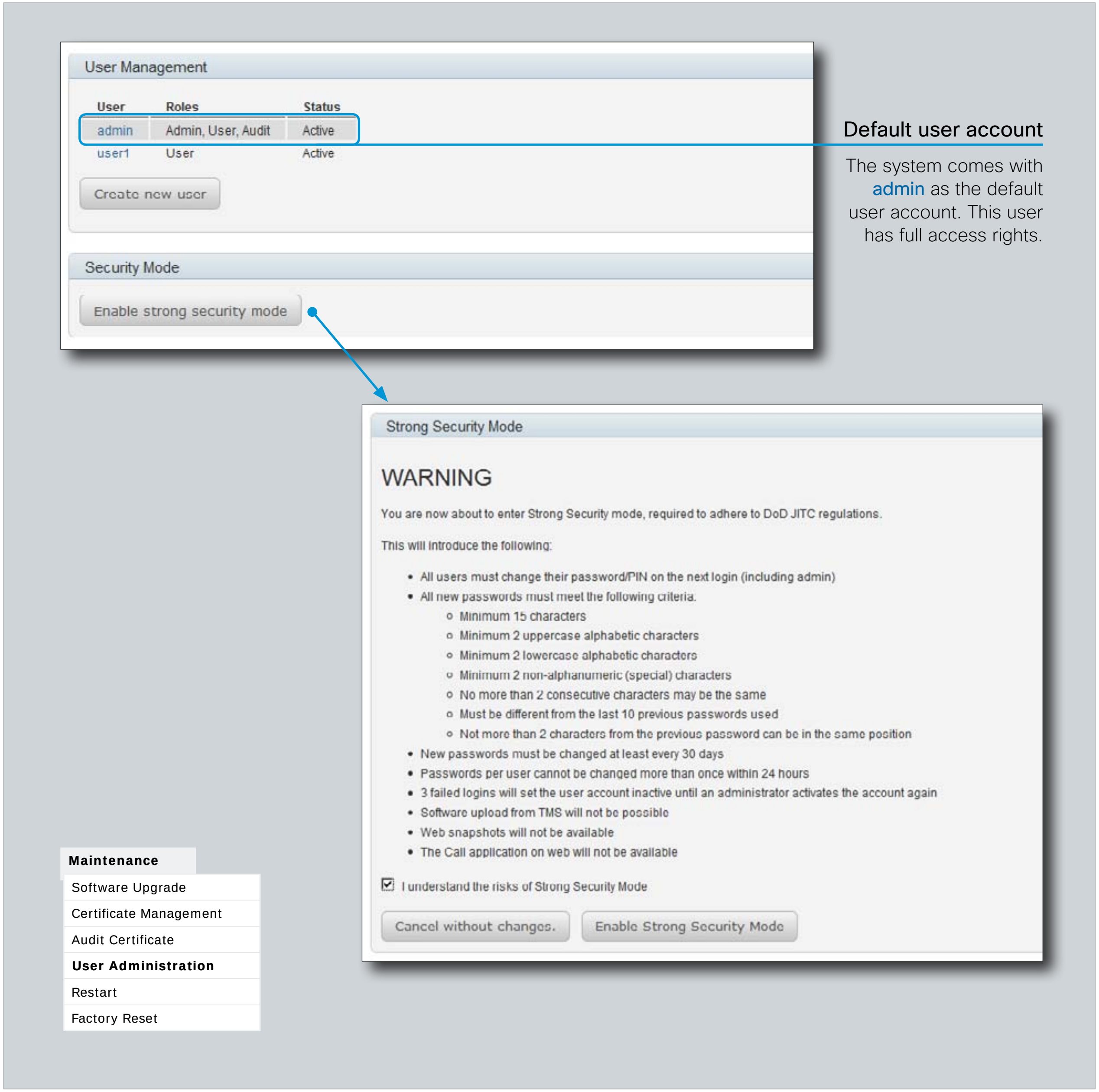
An administrator user account with full access rights, like the default admin user, must possess all the three roles.

Security mode

You can enable/disable the strong security mode from this page. You must read the warning carefully and check the *I understand the risks...* box before you can enable the strong security mode.

Strong security mode sets very strict password requirements, and requires all users to change their password on the next sign in.

Software upload from TMS, web snapshots and making calls from the web interface are prohibited in strong security mode.



User Management

User	Roles	Status
admin	Admin, User, Audit	Active
user1	User	Active

Security Mode

Default user account

The system comes with admin as the default user account. This user has full access rights.

Strong Security Mode

WARNING

You are now about to enter Strong Security mode, required to adhere to DoD JITC regulations.

This will introduce the following:

- All users must change their password/PIN on the next login (including admin)
- All new passwords must meet the following criteria:
  - Minimum 15 characters
  - Minimum 2 uppercase alphabetic characters
  - Minimum 2 lowercase alphabetic characters
  - Minimum 2 non-alphanumeric (special) characters
  - No more than 2 consecutive characters may be the same
  - Must be different from the last 10 previous passwords used
  - Not more than 2 characters from the previous password can be in the same position
- New passwords must be changed at least every 30 days
- Passwords per user cannot be changed more than once within 24 hours
- 3 failed logins will set the user account inactive until an administrator activates the account again
- Software upload from TMS will not be possible
- Web snapshots will not be available
- The Call application on web will not be available

☑ I understand the risks of Strong Security Mode

Creating a new user account

1. Press *Create new user*.
2. Fill in the Username, Password and PIN code, and select the user role(s) for this user account.

   As a default the user have to change the password and PIN code when signing in for the first time.

   Do not fill in the Distinguished Name (DN) Subject field unless you want to use certificate login on https.
3. Set the *Status* to **Active** to activate the user.
4. Press *Save* to save the changes.

Editing user details

1. Select the name of an existing user to open the Editing user window.
2. Edit the details.
3. Press *Save* to save the changes or *Cancel* to go back one step without storing the information.

Deactivating a user account

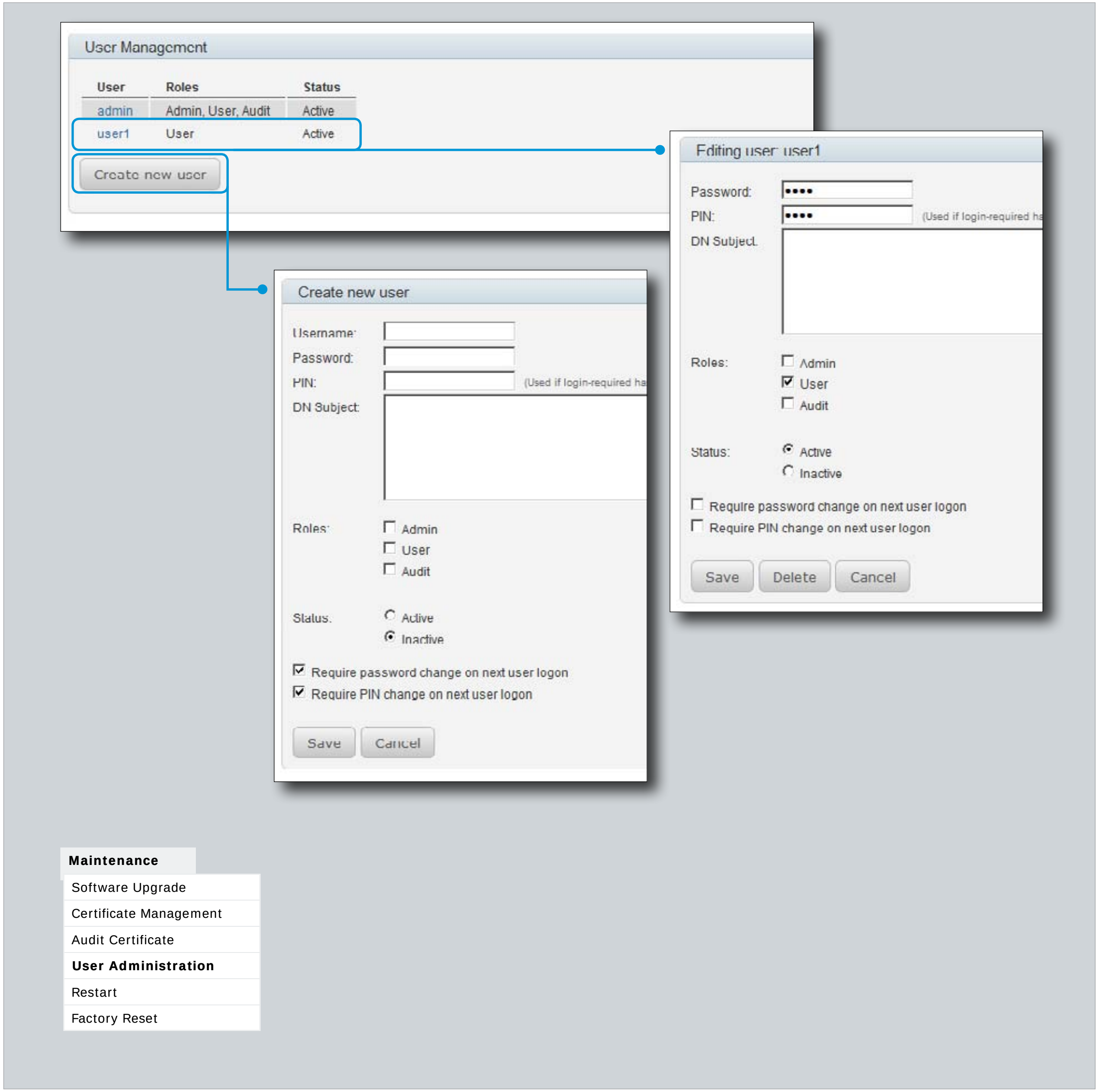
1. Select the name of an existing user to open the Editing user window.
2. Set the *Status* to **Inactive**.
3. Press *Save* to save the changes.

NOTE: Always keep at least one user with ADMIN rights **Active**.

Deleting a user account

1. Select the name of the user to open the Editing user window.
2. Press *Delete*.

NOTE: Always keep at least one user with ADMIN rights **Active**.



User Management

User	Roles	Status
admin	Admin, User, Audit	Active
user1	User	Active

Editing user: user1

Password: ••••
PIN: •••• (Used if login-required ha
DN Subject:
Roles: □ Admin ☑ User □ Audit
Status: ● Active ○ Inactive
□ Require password change on next user logon
□ Require PIN change on next user logon

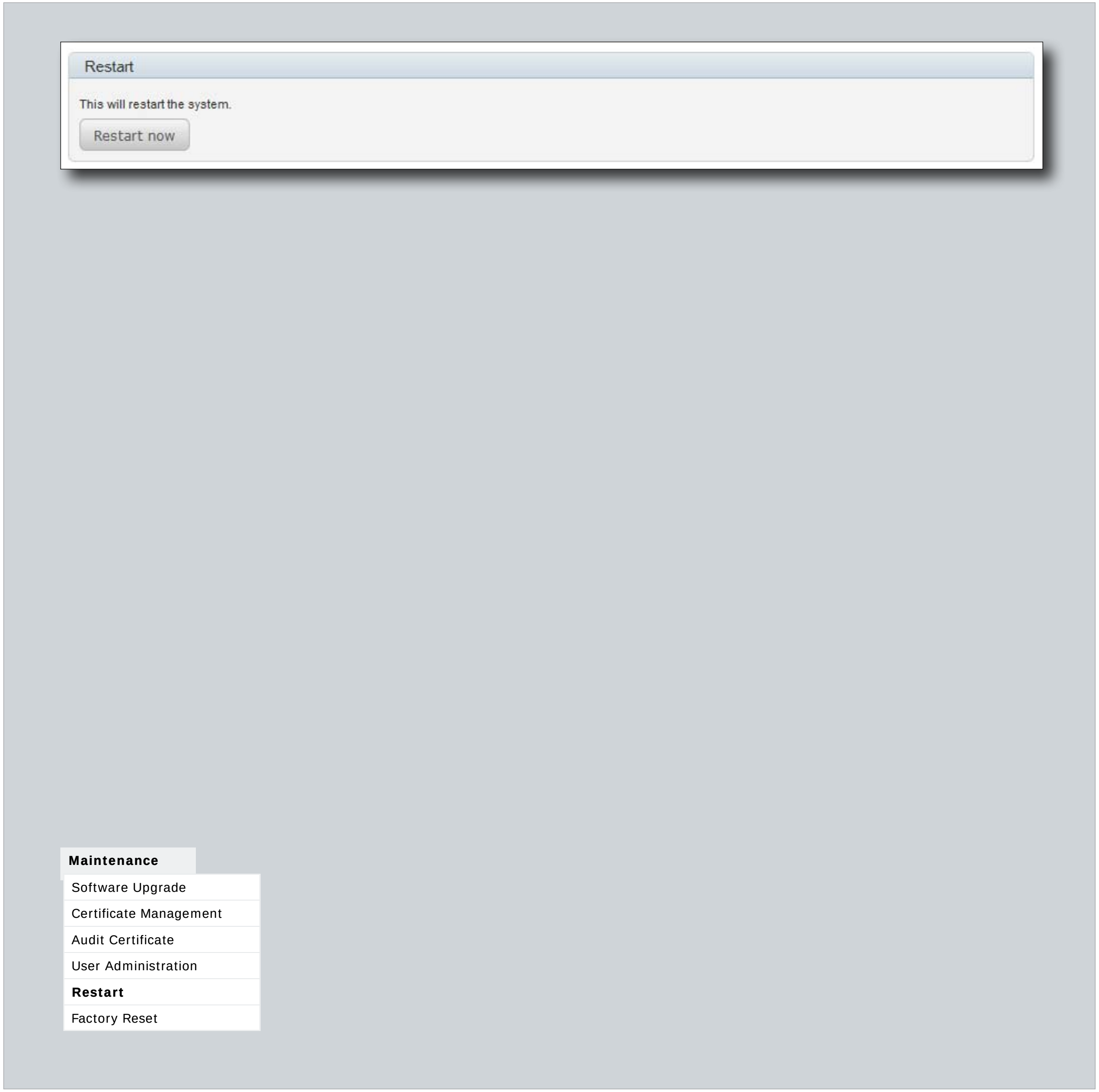
Create new user

Username:
Password:
PIN: (Used if login-required ha
DN Subject:
Roles: □ Admin □ User □ Audit
Status: ○ Active ● Inactive
☑ Require password change on next user logon
☑ Require PIN change on next user logon

Restarting the system

To restart the system, press *Restart now*.

Restarting the system takes a few minutes.



Restart

This will restart the system.

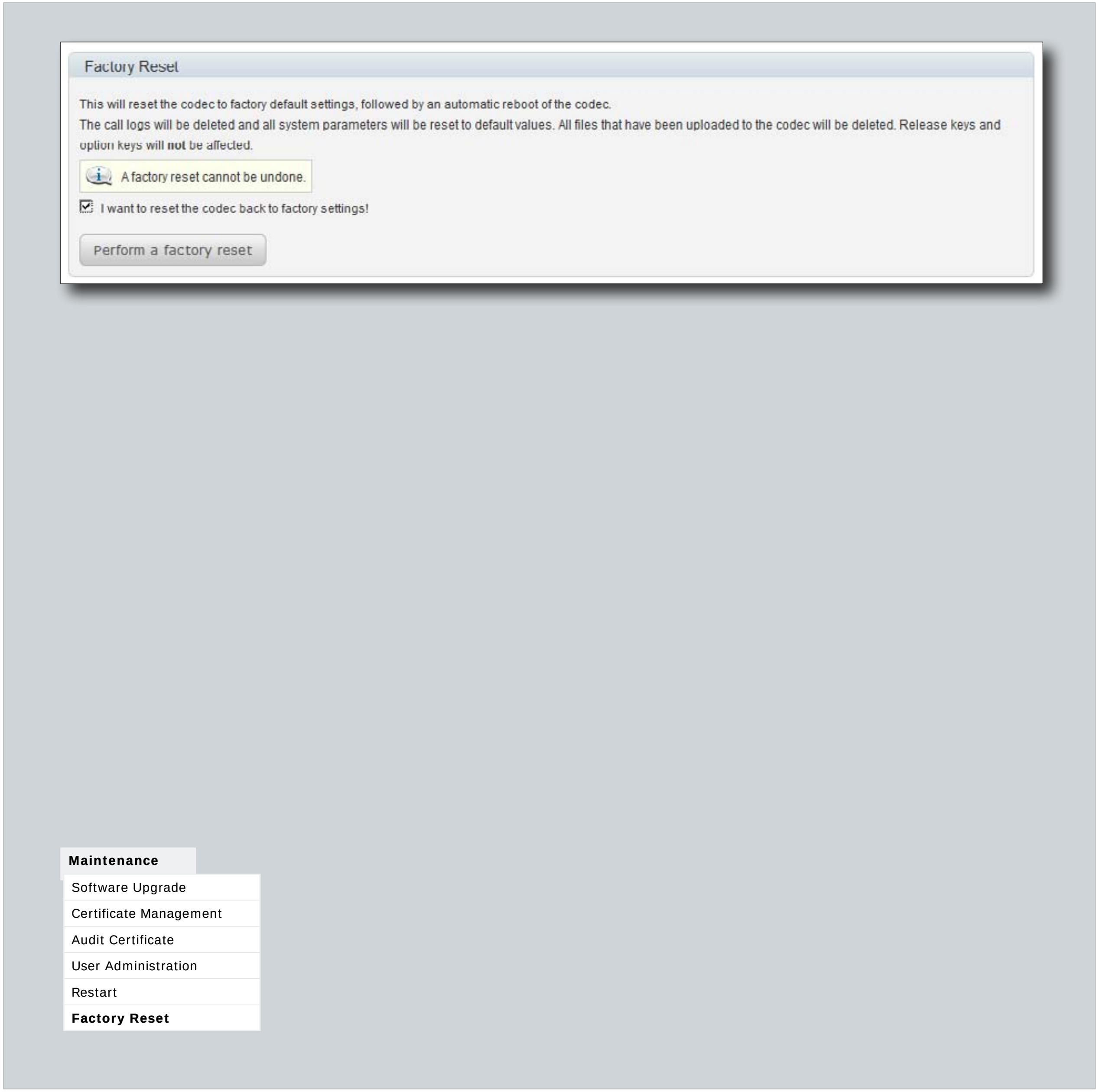
Factory reset

When performing a factory reset the call logs will be deleted and all system parameters will be reset to default values. All files that have been uploaded to the codec will be deleted. Release keys and option keys will be preserved.

NOTE: It is **not** possible to undo a factory reset.

Read the provided information carefully before you perform a factory reset. Then check the *I want to reset...* box, and finally press *Perform a factory reset*.

Wait while the system resets. The system will reboot automatically when finished.



Factory Reset

This will reset the codec to factory default settings, followed by an automatic reboot of the codec.

The call logs will be deleted and all system parameters will be reset to default values. All files that have been uploaded to the codec will be deleted. Release keys and option keys will **not** be affected.

A factory reset cannot be undone.

☑ I want to reset the codec back to factory settings!

Chapter 3

The advanced settings

Overview of the advanced settings

In the following pages you will find a complete list of the system settings which are configured from the *Advanced configuration* menu on screen or the *Advanced Configuration* page on the web interface.

The examples show either the default value or an example of a value.

Find the IP address of your system

The IPv4 or IPv6 address of your system is included in the *System Information* list. You can find this list either using the remote control and on-screen menu (navigate to *Home > Settings > System Information*) or using the Touch controller (tap *More > Settings > System Information*).

Open the web interface

Open a web browser and enter your video conference system's IP address in the address bar; then sign in.

The Audio settings

Audio Microphones Mute Enabled

Determine whether audio-mute is allowed or not. The default value is True.

Requires user role: ADMIN

Value space: `<True/InCallOnly>`

True: Muting of audio is always available.

InCallOnly: Muting of audio is only available when the device is in a call. When Idle it is not possible to mute the microphone. This is useful when an external telephone service/audio system is connected via the codec and is to be available when the codec is not in a call. When set to InCallOnly this will prevent the audio-system from being muted by mistake.

Example: `Audio Microphones Mute Enabled: True`

Audio SoundsAndAlerts KeyTones Mode

The system can produce a sound every time a key on the remote control is pressed.

Requires user role: USER

Value space: `<On/Off>`

On: There will be a sound indicator when pressing keys on the remote control.

Off: The remote control Key Tones is switched off.

Example: `Audio SoundsAndAlerts KeyTones Mode: Off`

Audio SoundsAndAlerts RingTone

Select the ring tone for incoming calls.

Requires user role: USER

Value space: `<Marbles/IceCrystals/Polaris/Alert/Discreet/Fantasy/Jazz/Nordic/Echo/Rhythmic>`

Range: Select a tone from the list of ring tones.

Example: `Audio SoundsAndAlerts RingTone: Jazz`

Audio SoundsAndAlerts RingVolume

Sets the ring tone volume for an incoming call.

Requires user role: USER

Value space: `<0..100>`

Range: The value goes in steps of 5 from 0 to 100 (from -34.5 dB to 15 dB). Volume 0 = Off.

Example: `Audio SoundsAndAlerts RingVolume: 50`

Audio Volume

Set the volume on the loudspeaker.

Requires user role: USER

Value space: `<0..100>`

Range: The value goes in steps of 5 from 0 to 100 (from -34.5 dB to 15 dB). Value 0 = Off.

Example: `Audio Volume: 70`

The Cameras settings

Cameras PowerLine Frequency

Applies to cameras supporting PowerLine frequency anti-flickering, i.e PrecisionHD 1080p cameras.

Requires user role: ADMIN

Value space: `<Auto/50Hz/60Hz>`

Auto: Set to Auto to enable power frequency auto detection in the camera.
50Hz: Set to 50 Hz.
60Hz: Set to 60 Hz.

Example: `Cameras PowerLine Frequency: Auto`

Cameras Camera [1..1] Backlight

This configuration turns backlight compensation on or off. Backlight compensation is useful when there is much light behind the persons in the room. Without compensation the persons will easily appear very dark to the far end.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Turn on the camera backlight compensation.
Off: Turn off the camera backlight compensation.

Example: `Cameras Camera 1 Backlight: Off`

Cameras Camera [1..1] Brightness Mode

Set the camera brightness mode.

Requires user role: ADMIN

Value space: `<Auto/Manual>`

Auto: The camera brightness is automatically set by the system.
Manual: Enable manual control of the camera brightness, e.g. the level of the brightness level setting will be used for the camera.

Example: `Cameras Camera 1 Brightness Mode: Auto`

Cameras Camera [1..1] Brightness Level

Set the brightness level. NOTE: Requires the Camera Brightness Mode to be set to Manual.

Requires user role: ADMIN

Value space: `<1..31>`

Range: Select a value from 1 to 31.

Example: `Cameras Camera 1 Brightness Level: 1`

Cameras Camera [1..1] Flip

With Flip mode (vertical flip) you can flip the image upside down.

Requires user role: ADMIN

Value space: `<Auto/On/Off>`

Auto: When the camera is placed upside down the image is automatically flipped upside down. This setting will only take effect for a camera that automatically detects which way it is mounted.
On: When enabled the video on screen is flipped. This setting is used when a camera is mounted upside down, but cannot automatically detect which way it is mounted.
Off: Display the video on screen the normal way.

Example: `Cameras Camera 1 Flip: Off`

Cameras Camera [1..1] Focus Mode

Set the camera focus mode.

Requires user role: ADMIN

Value space: `<Auto/Manual>`

Auto: The camera will auto focus once a call is connected, as well as after moving the camera (pan, tilt, zoom). The system will use auto focus only for a few seconds to set the right focus; then auto focus is turned off to prevent continuous focus adjustments of the camera.
Manual: Turn the autofocus off and adjust the camera focus manually.

Example: `Cameras Camera 1 Focus Mode: Auto`

Cameras Camera [1..1] Gamma Mode

Applies to cameras which support gamma mode. The Gamma Mode setting enables for gamma corrections. Gamma describes the nonlinear relationship between image pixels and monitor brightness. The Cisco TelePresence PrecisionHD 720p camera supports gamma mode. The PrecisionHD 1080p camera does not support gamma mode.

Requires user role: ADMIN

Value space: `<Auto/Manual>`

Auto: Auto is the default and the recommended setting.
Manual: In severe light conditions, you may switch mode to manual and specify explicitly which gamma table to use by setting the Gamma Level.

Example: `Cameras Camera 1 Gamma Mode: Auto`

Cameras Camera [1..1] Gamma Level

By setting the Gamma Level you can select which gamma correction table to use. This setting may be useful in difficult lighting conditions, where changes to the brightness setting does not provide satisfactory results. NOTE: Requires the Gamma Mode to be set to Manual.

Requires user role: ADMIN

Value space: `<0..7>`

Range: Select a value from 0 to 7.

Example: `Cameras Camera 1 Gamma Level: 0`

Cameras Camera [1..1] IrSensor

The IR sensor LED is located in the front of the camera and flickers when the IR sensor is activated from the remote control. Both the Codec C Series and PrecisionHD camera have IR sensors, and only one of them needs to be enabled at the time.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable the IR sensor on the camera.
Off: Disable the IR sensor on the camera.

Example: `Cameras Camera 1 IrSensor: On`

Cameras Camera [1..1] Mirror

With Mirror mode (horizontal flip) you can mirror the image on screen.

Requires user role: ADMIN

Value space: `<Auto/On/Off>`

Auto: When the camera is placed upside down the image is automatically mirrored. Use this setting with cameras that can be mounted upside down, and that can auto detect that the camera is mounted upside down.
On: See the selfview in mirror mode, e.g. the selfview is reversed and the experience of selfview is as seeing yourself in a mirror.
Off: See the selfview in normal mode, e.g. the experience of selfview is as seeing yourself as other people see you.

Example: `Cameras Camera 1 Mirror: Off`

Cameras Camera [1..1] Whitebalance Mode

Set the camera whitebalance mode.

Requires user role: ADMIN

Value space: `<Auto/Manual>`

Auto: The camera will continuously adjust the whitebalance depending on the camera view.
Manual: Enables manual control of the camera whitebalance, e.g. the level of the whitebalance level setting will be used for the camera.

Example: `Cameras Camera 1 Whitebalance Mode: Auto`

Cameras Camera [1..1] Whitebalance Level

Set the whitebalance level. NOTE: Requires the Camera Whitebalance Mode to be set to manual.

Requires user role: ADMIN

Value space: `<1..16>`

Range: Select a value from 1 to 16.

Example: `Cameras Camera 1 Whitebalance Level: 1`

Cameras Camera [1..1] DHCP

Applies to cameras which support DHCP. The Cisco TelePresence PrecsisionHD 1080p camera supports DHCP. The camera must be connected to a LAN. When set, the command enables support for SW upgrade of daisy chained cameras. It will enable the camera's DHCP function and force start of MAC and IP address retrieval. Remember to reset the DHCP when the camera is no longer connected to a LAN.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable DHCP in the camera. The camera is automatically re-booted. After re-boot the DHCP is started and the IP address will be retrieved. Run the commnand " xStatus Camera" for result.
Off: Disable DHCP in the camera. NOTE: This setting should be applied when the camera is not connected to a LAN.

Example: `Cameras Camera 1 DHCP: Off`

The Conference settings

Conference [1..1] AutoAnswer Mode

Set the AutoAnswer mode.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable AutoAnswer to let the system automatically answer all incoming calls.
Off: The incoming calls must be answered manually by pressing the OK key or the green Call key on the remote control.

Example: `Conference 1 AutoAnswer Mode: Off`

Conference [1..1] AutoAnswer Mute

Determine if the microphone shall be muted when an incoming call is automatically answered. NOTE: Requires the AutoAnswer Mode to be enabled.

Requires user role: ADMIN

Value space: `<On/Off>`

On: The incoming call will be muted when automatically answered.
Off: The incoming call will not be muted.

Example: `Conference 1 AutoAnswer Mute: Off`

Conference [1..1] AutoAnswer Delay

Define how long (in seconds) an incoming call has to wait before it is answered automatically by the system. NOTE: Requires the AutoAnswer Mode to be enabled.

Requires user role: ADMIN

Value space: `<0..50>`

Range: Select a value from 0 to 50 seconds.

Example: `Conference 1 AutoAnswer Delay: 0`

Conference [1..1] MicUnmuteOnDisconnect Mode

Determine if the microphones shall be unmuted automatically when all calls are disconnected. In a meeting room or other shared resources this could be done to prepare the system for the next user.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Un-mute the microphones after the call is disconnected.
Off: If muted, let the microphones remain muted after the call is disconnected.

Example: `Conference 1 MicUnmuteOnDisconnect Mode: On`

Conference [1..1] DoNotDisturb Mode

Determine if there should be an alert on incoming calls.

Requires user role: USER

Value space: `<On/Off/Timed>`

On: All incoming calls will be rejected and they will be registered as missed calls. The calling side will receive a busy signal. A message telling that Do Not Disturb is switched on will display on the Touch controller or main display. The calls received while in Do Not Disturb mode will be shown as missed calls.
Off: The incoming calls will come through as normal.
Timed: Select this option when using the API to switch Do Not Disturb mode on and off (xCommand Conference DoNotDisturb Activate and xCommand Conference DoNotDisturb Deactivate).

Example: `DoNotDisturb Mode: Off`

Conference [1..1] FarEndControl Mode

Lets you decide if the remote side (far end) should be allowed to select your video sources and control your local camera (pan, tilt, zoom).

Requires user role: ADMIN

Value space: `<On/Off>`

On: Allows the far end to be able to select your video sources and control your local camera (pan, tilt, zoom). You will still be able to control your camera and select your video sources as normal.
Off: The far end is not allowed to select your video sources or to control your local camera (pan, tilt, zoom).

Example: `Conference 1 FarEndControl Mode: On`

Conference [1..1] FarEndControl SignalCapability

Set the far end control (H.224) signal capability mode.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable the far end control signal capability.
Off: Disable the far end control signal capability.

Example: `Conference 1 FarEndControl SignalCapability: On`

Conference [1..1] Encryption Mode

Set the conference encryption mode. A padlock with the text " Encryption On" or " Encryption Off" displays on screen for a few seconds when the conference starts.

Requires user role: ADMIN

Value space: `<BestEffort/On/Off>`

BestEffort: The system will use encryption whenever possible.

> *In Point to point calls:* If the far end system supports encryption (AES-128), the call will be encrypted. If not, the call will proceed without encryption.

> *In MultiSite calls:* In order to have encrypted MultiSite conferences, all sites must support encryption. If not, the conference will be unencrypted.

On: The system will only allow calls that are encrypted.

Off: The system will not use encryption.

Example: `Conference 1 Encryption Mode: BestEffort`

Conference [1..1] DefaultCall Protocol

Set the Default Call Protocol to be used when placing calls from the system.

Requires user role: ADMIN

Value space: `<H323/Sip>`

H.323: Select H.323 to ensure that calls are set up as H.323 calls.

Sip: Select SIP to ensure that calls are set up as SIP calls.

Example: `Conference 1 DefaultCall Protocol: H323`

Conference [1..1] DefaultCall Rate

Set the Default Call Rate to be used when placing calls from the system.

Requires user role: ADMIN

Value space: `<64..6000>`

Range: Select a value between 64 and 6000 kbps

Example: `Conference 1 DefaultCall Rate: 768`

Conference [1..1] MaxTransmitCallRate

Specify the maximum transmit call rate to be used when placing or receiving calls.

Requires user role: ADMIN

Value space: `<64..6000>`

Range: Select a value between 64 and 6000 kbps.

Example: `Conference 1 MaxTransmitCallRate: 6000`

Conference [1..1] MaxReceiveCallRate

Specify the maximum receive call rate to be used when placing or receiving calls.

Requires user role: ADMIN

Value space: `<64..6000>`

Range: Select a value between 64 and 6000 kbps.

Example: `Conference 1 MaxReceiveCallRate: 6000`

Conference [1..1] VideoBandwidth Mode

Set the conference video bandwidth mode.

Requires user role: ADMIN

Value space: `<Dynamic/Static>`

Dynamic: The available transmit bandwidth for the video channels are distributed among the currently active channels. If there is no presentation, the main video channels will use the bandwidth of the presentation channel.

Static: The available transmit bandwidth is assigned to each video channel, even if it is not active.

Example: `Conference 1 VideoBandwidth Mode: Dynamic`

Conference [1..1] VideoBandwidth MainChannel Weight

The available transmit video bandwidth is distributed on the main channel and presentation channel according to " MainChannel Weight" and " PresentationChannel Weight". If the main channel weight is 2 and the presentation channel weight is 1, then the main channel will use twice as much bandwidth as the presentation channel.

Requires user role: ADMIN

Value space: `<1..10>`

Range: 1 to 10.

Example: `Conference 1 VideoBandwidth MainChannel Weight: 5`

Conference [1..1] VideoBandwidth PresentationChannel Weight

The available transmit video bandwidth is distributed on the main channel and presentation channel according to " MainChannel Weight" and " PresentationChannel Weight". If the main channel weight is 2 and the presentation channel weight is 1, then the main channel will use twice as much bandwidth as the presentation channel.

Requires user role: ADMIN

Value space: `<1..10>`

Range: 1 to 10.

Example: `Conference 1 VideoBandwidth PresentationChannel Weight: 5`

Conference [1..1] PacketLossResilience Mode

Set the packetloss resilience mode. This configuration will only take effect for calls initiated after the configuration is set.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable the packetloss resilience.
Off: Disable the packetloss resilience.

Example: `Conference 1 PacketLossResilience Mode: On`

Conference [1..1] Presentation Policy

Control how the presentation service is to be performed.

Requires user role: ADMIN

Value space: `<LocalRemote/LocalOnly>`

LocalRemote: The presentation will be shown locally and sent to remote side.
LocalOnly: The presentation will only be shown locally.

Example: `Conference 1 Presentation Policy: LocalRemote`

Conference [1..1] Multipoint Mode

Define how the video system handles multipoint video conferences. Basically there are two ways: The video system can use its built-in MultiSite feature (optional), or it can rely on the MultiWay network solution. MultiWay requires that your video network includes an external Multipoint control unit (MCU). The MultiSite feature allows up to four participants (yourself included) plus one additional audio call. An External MCU may let you set up conferences with many participants.

Requires user role: ADMIN

Value space: `<Off/MulitSite/MultiWay/Auto>`

Off: Multipoint conferences are not allowed.
MultiSite: Use MultiSite for multipoint conferences. If MultiSite is chosen when the MultiSite feature is not available, the Multipoint Mode will be set to Off.
MultiWay: Use MultiWay for multipoint conferences. The Multipoint Mode will be set to Off automatically if the MultiWay service is unavailable, e.g. when a server address is not specified in the NetworkServices MultiWay Address setting.
Auto: If a MultiWay address is specified in the NetworkServices Multiway Address setting, MultiWay takes priority over MultiSite. If neither MultiWay nor MultiSite is available, the multipoint mode is set to Off automatically.

Example: `Conference 1 Multipoint Mode: Auto`

Conference [1..1] IncomingMultisiteCall Mode

Select whether or not to allow incoming calls when already in a call/conference.

Requires user role: ADMIN

Value space: `<Allow/Deny>`

Allow: You will be notified when someone calls you while you are already in a call. You can accept the incoming call or not. The ongoing call may be put on hold while answering the incoming call; or you may merge the calls (requires MultiSite or MultiWay support).
Deny: An incoming call will be rejected if you are already in a call. You will not be notified about the incoming call. However, the call will appear as a missed call in the call history list.

Example: `Conference 1 IncomingMultisiteCall Mode: Allow`

The FacilityService settings

FacilityService Service [1..5] Type

Up to five different facility services can be supported simultaneously. With this setting you can select what kind of services they are.

A facility service is not available unless both the FacilityService Service Name and the FacilityService Service Number settings are properly set.

Only FacilityService Service 1 with Type Helpdesk is available on the Touch controller. Facility services are not available when using the remote control and on-screen menu.

Requires user role: ADMIN

Value space: `<Other/Concierge/Helpdesk/Emergency/Security/Catering/Transportation>`

Other: Select this option for services not covered by the other options.
Concierge: Select this option for concierge services.
Helpdesk: Select this option for helpdesk services.
Emergency: Select this option for emergency services.
Security: Select this option for security services.
Catering: Select this option for catering services.
Transportation: Select this option for transportation services.

Example: `FacilityService Service 1 Type: Helpdesk`

FacilityService Service [1..5] Name

Set the name of each facility service. Up to five different facility services are supported.

A facility service is not available unless both the FacilityService Service Name and the FacilityService Service Number settings are properly set.

Only FacilityService Service 1 is available on the Touch controller, and its Name is used on the facility service call button. Facility services are not available when using the remote control and on-screen menu.

Requires user role: ADMIN

Value space: `<S: 0, 255>`

Format: String with a maximum of 255 characters.

Example: `FacilityService Service 1 Name: ""`

FacilityService Service [1..5] Number

Set the number for each facility service. Up to five different facility services are supported.

A facility service is not available unless both the FacilityService Service Name and the FacilityService Service Number settings are properly set.

Only FacilityService Service 1 is available on the Touch controller. Facility services are not available when using the remote control and on-screen menu.

Requires user role: ADMIN

Value space: `<S: 0, 255>`

Format: String with a maximum of 255 characters.

Example: `FacilityService Service 1 Number: ""`

FacilityService Service [1..5] CallType

Set the call type for each facility service. Up to five different facility services are supported.

A facility service is not available unless both the FacilityService Service Name and the FacilityService Service Number settings are properly set.

Only FacilityService Service 1 is available on the Touch controller. Facility services are not available when using the remote control and on-screen menu.

Requires user role: ADMIN

Value space: `<Video/Audio>`

Video: Select this option for video calls.
Audio: Select this option for audio calls.

Example: `FacilityService Service 1 CallType: Video`

The H323 settings

H323 NAT Mode

The firewall traversal technology creates a secure path through the firewall barrier, and enables proper exchange of audio/video data when connected to an external video conferencing system (when the IP traffic goes through a NAT router). NOTE: NAT does not work in conjunction with gatekeepers.

Requires user role: ADMIN

Value space: `<Auto/On/Off>`

Auto: The system will determine if the " NAT Address" or the real IP-address should be used within signalling. This is done to make it possible to place calls to endpoints on the LAN as well as endpoints on the WAN.

On: The system will signal the configured " NAT Address" in place of its own IP-address within Q.931 and H.245. The NAT Server Address will be shown in the startup-menu as: " My IP Address: 10.0.2.1".

Off: The system will signal the real IP Address.

Example: `H323 NAT Mode: Off`

H323 NAT Address

Enter the external/global IP-address to the router with NAT support. Packets sent to the router will then be routed to the system.

In the router, the following ports must be routed to the system's IP-address:

* Port 1720

* Port 5555-5574

* Port 2326-2485

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: String with a maximum of 64 characters.

Example: `H323 NAT Address: ""`

H323 Profile [1..1] Authentication Mode

Set the authenticatin mode for the H.323 profile.

Requires user role: ADMIN

Value space: `<On/Off>`

On: If the H.323 Gatekeeper Authentication Mode is set to On and a H.323 Gatekeeper indicates that it requires authentication, the system will try to authenticate itself to the gatekeeper. NOTE: Requires the Authentication LoginName and Authentication Password to be defined on both the codec and the Gatekeeper.

Off: If the H.323 Gatekeeper Authentication Mode is set to Off the system will not try to authenticate itself to a H.323 Gatekeeper, but will still try a normal registration.

Example: `H323 Profile 1 Authentication Mode: Off`

H323 Profile [1..1] Authentication LoginName

The system sends the Authentication Login Name and the Authentication Password to a H.323 Gatekeeper for authentication. The authentication is a one way authentication from the codec to the H.323 Gatekeeper, i.e. the system is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the system will still try to register. NOTE: Requires the H.323 Gatekeeper Authentication Mode to be enabled.

Requires user role: ADMIN

Value space: `<S: 0, 50>`

Format: String with a maximum of 50 characters.

Example: `H323 Profile 1 Authentication LoginName: ""`

H323 Profile [1..1] Authentication Password

The system sends the Authentication Login Name and the Authentication Password to a H.323 Gatekeeper for authentication. The authentication is a one way authentication from the codec to the H.323 Gatekeeper, i.e. the system is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the system will still try to register. NOTE: Requires the H.323 Gatekeeper Authentication Mode to be enabled.

Requires user role: ADMIN

Value space: `<S: 0, 50>`

Format: String with a maximum of 50 characters.

Example: `H323 Profile 1 Authentication Password:`

H323 Profile [1..1] CallSetup Mode

The H.323 Call Setup Mode defines whether to use a Gatekeeper or Direct calling when establishing H323 calls.

NOTE: Direct H.323 calls can be made even though the H.323 Call Setup Mode is set to Gatekeeper.

Requires user role: ADMIN

Value space: `<Direct/Gatekeeper>`

Direct: An IP-address must be used when dialling in order to make the H323 call.

Gatekeeper: The system will use a Gatekeeper to make a H.323 call. When selecting this option the H323 Profile Gatekeeper Address and H323 Profile Gatekeeper Discovery settings must also be configured.

Example: `H323 Profile 1 CallSetup Mode: Gatekeeper`

H323 Profile [1..1] Gatekeeper Discovery

Determine how the system shall register to a H.323 Gatekeeper.

Requires user role: ADMIN

Value space: `<Manual/Auto>`

Manual: The system will use a specific Gatekeeper identified by the Gatekeeper's IP-address.

Auto: The system will automatically try to register to any available Gatekeeper. If a Gatekeeper responds to the request sent from the codec within 30 seconds this specific Gatekeeper will be used. This requires that the Gatekeeper is in auto discovery mode as well. If no Gatekeeper responds, the system will not use a Gatekeeper for making H.323 calls and hence an IP-address must be specified manually.

Example: `H323 Profile 1 Gatekeeper Discovery: Manual`

H323 Profile [1..1] Gatekeeper Address

Enter the IP address of the Gatekeeper. NOTE: Requires the H.323 Call Setup Mode to be set to Gatekeeper and the Gatekeeper Discovery to be set to Manual.

Requires user role: ADMIN

Value space: `<S: 0, 255>`

Format: Only the valid IP address format is accepted. An IP address that contains letters (192.a.2.0) or unvalid IP addresses (192.0.1234.0) will be rejected.

Example: `H323 Profile 1 Gatekeeper Address: "192.0.2.0"`

H323 Profile [1..1] H323Alias E164

The H.323 Alias E.164 defines the address of the system, according to the numbering plan implemented in the H.323 Gatekeeper. The E.164 alias is equivalent to a telephone number, sometimes combined with access codes.

Requires user role: ADMIN

Value space: `<S: 0, 30>`

Format: Compact string with a maximum of 30 characters. Valid characters are 0-9, * and #.

Example: `H323 Profile 1 H323Alias E164: "90550092"`

H323 Profile [1..1] H323Alias ID

Lets you specify the H.323 Alias ID which is used to address the system on a H.323 Gatekeeper and will be displayed in the call lists. Example: " firstname.surname@company.com", " My H.323 Alias ID"

Requires user role: ADMIN

Value space: `<S: 0, 49>`

Format: String with a maximum of 49 characters

Example: `H323 Profile 1 H323Alias ID: "firstname.surname@company.com"`

H323 Profile [1..1] PortAllocation

The H.323 Port Allocation setting affects the H.245 port numbers used for H.323 call signalling.

Requires user role: ADMIN

Value space: `<Dynamic/Static>`

Dynamic: The system will allocate which ports to use when opening a TCP connection. The reason for doing this is to avoid using the same ports for subsequent calls, as some firewalls consider this as a sign of attack. When Dynamic is selected, the H.323 ports used are from 11000 to 20999. Once 20999 is reached they restart again at 11000. For RTP and RTCP media data, the system is using UDP ports in the range 2326 to 2487. Each media channel is using two adjacent ports, ie 2330 and 2331 for RTP and RTCP respectively. The ports are automatically selected by the system within the given range. Firewall administrators should not try to deduce which ports are used when, as the allocation schema within the mentioned range may change without any further notice.

Static: When set to Static the ports are given within a static predefined range [5555-6555].

Example: `H323 Profile 1 PortAllocation: Dynamic`

The Network settings

Network [1..1] Assignment

Define whether to use DHCP or Static IPv4 assignment.

Requires user role: ADMIN

Value space: `<Static/DHCP>`

Static: Set the network assignment to Static and configure the static IPv4 settings (IP Address, SubnetMask and Gateway).
DHCP: The system addresses are automatically assigned by the DHCP server.

Example: `Network 1 Assignment: DHCP`

Network [1..1] DNS Domain Name

DNS Domain Name is the default domain name suffix which is added to unqualified names.

Example: If the DNS Domain Name is " company.com" and the name to lookup is " MyVideoSystem", this will result in the DNS lookup " MyVideoSystem.company.com".

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: String with a maximum of 64 characters.

Example: `Network 1 DNS Domain Name: ""`

Network [1..1] DNS Server [1..5] Address

Define the network addresses for DNS servers. Up to 5 addresses may be specified. If the network addresses are unknown, contact your administrator or Internet Service Provider.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: String with a maximum of 64 characters.

Example: `Network 1 DNS Server 1 Address: ""`

Network [1..1] IPStack

Select which internet protocols the system will support.

Requires user role: ADMIN

Value space: `<IPv4/IPv6>`

IPv4: IP version 4 is supported.
IPv6: IP version 6 is supported. The IPv4 settings (IP Address, IP Subnet Mask and Gateway) will be disabled.

Example: `Network 1 IPStack: IPv4`

Network [1..1] IPv4 Address

Enter the static IPv4 network address for the system. Only applicable if the Network Assignment is set to Static.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: Only the valid IP address format is accepted. An IP address that contains letters (192.a.2.0) or unvalid IP addresses (192.0.1234.0) will be rejected.

Example: `Network 1 IPv4 Address: "192.0.2.0"`

Network [1..1] IPv4 Gateway

Define the IPv4 network gateway. Only applicable if the Network Assignment is set to Static.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: Compact string with a maximum of 64 characters.

Example: `Network 1 IPv4 Gateway: "192.0.2.0"`

Network [1..1] IPv4 SubnetMask

Define the IPv4 network subnet mask. Only applicable if the Network Assignment is set to Static.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: Compact string with a maximum of 64 characters.

Example: `Network 1 IPv4 SubnetMask: "255.255.255.0"`

Network [1..1] IPv6 Address

Enter the static IPv6 network address for the system. Only applicable if the Network IPv6 Assignment is set to Static.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: The IPv6 address of host name.

Example: `Network 1 IPv6 Address: "ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff"`

Network [1..1] IPv6 Gateway

Define the IPv6 network gateway address. Only applicable if the Network IPv6 Assignment is set to Static.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: The IPv6 address of host name.

Example: `Network 1 IPv6 Gateway: "ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff"`

Network [1..1] IPv6 Assignment

Define whether to use Autoconf or Static IPv6 assignment.

Requires user role: ADMIN

Value space: `<Static/Autoconf>`

Static: Set the network assignment to Static and configure the static IPv6 settings (IP Address and Gateway).

Autoconf: Enable IPv6 stateless autoconfiguration of the IPv6 network interface. See RFC4862 for a detailed description.

Example: `Network 1 IPv6 Assignment: Autoconf`

Network [1..1] IPv6 DHCPOptions

Retrieves a set of DHCP options from a DHCPv6 server.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable the retrieval of a selected set of DHCP options from a DHCPv6 server.

Off: Set to Off when IPv6 Assignment is set to Static.

Example: `Network 1 IPv6 Gateway: On`

Network [1..1] QoS Mode

The QoS (Quality of Service) is a method which handles the priority of audio, video and data in the network. The QoS settings must be supported by the infrastructure. Diffserv (Differentiated Services) is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing QoS priorities on modern IP networks.

Requires user role: ADMIN

Value space: `<Off/Diffserv>`

Off: No QoS method is used.

Diffserv: When you set the QoS Mode to Diffserv you must configure the Diffserv sub menu settings (Audio, Data, Signalling and Video).

Example: `Network 1 QoS Mode: diffserv`

Network [1..1] QoS Diffserv Audio

The Diffserv Audio defines which priority Audio packets should have in an IP network. Enter a priority, which ranges from 0 to 63 for the packets. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator. NOTE: Requires the Network QoS Mode to be set to Diffserv.

Requires user role: ADMIN

Value space: `<0..63>`

Audio: A recommended value is Diffserv Code Point (DSCP) AF41, which equals the value 34. If in doubt, contact your network administrator.

Range: Select a value from 0 to 63.

Example: `Network 1 QoS Diffserv Audio: 0`

Network [1..1] QoS Diffserv Data

The Diffserv Data defines which priority Data packets should have in an IP network. Enter a priority, which ranges from 0 to 63 for the packets. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator. NOTE: Requires the Network QoS Mode to be set to Diffserv.

Requires user role: ADMIN

Value space: `<0..63>`

Data: A recommended value is Diffserv Code Point (DSCP) AF23, which equals the value 22. If in doubt, contact your network administrator.

Range: Select a value from 0 to 63.

Example: `Network 1 QoS Diffserv Data: 0`

Network [1..1] QoS Diffserv Signalling

The Diffserv Signalling defines which priority Signalling packets should have in an IP network. Enter a priority, which ranges from 0 to 63 for the packets. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator. NOTE: Requires the Network QoS Mode to be set to Diffserv.

Requires user role: ADMIN

Value space: `<0..63>`

Signalling: A recommended value is Diffserv Code Point (DSCP) AF31, which equals the value 26. If in doubt, contact your network administrator.

Range: Select a value from 0 to 63.

Example: `Network 1 QoS Diffserv Signalling: 0`

Network [1..1] QoS Diffserv Video

The Diffserv Video defines which priority Video packets should have in an IP network. Enter a priority, which ranges from 0 to 63 for the packets. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator. NOTE: Requires the Network QoS Mode to be set to Diffserv.

Requires user role: ADMIN

Value space: `<0..63>`

Video: A recommended value is Diffserv Code Point (DSCP) AF41, which equals the value 34. If in doubt, contact your network administrator.
Range: Select a value from 0 to 63.

Example: `Network 1 QoS Diffserv Video: 0`

Network [1..1] IEEE8021X Mode

The system can be connected to an IEEE 802.1X LAN network, with a port-based network access control that is used to provide authenticated network access for Ethernet networks.

Requires user role: ADMIN

Value space: `<On/Off>`

On: The 802.1X authentication is enabled.
Off: The 802.1X authentication is disabled (default).

Example: `Network 1 IEEE8021X Mode: Off`

Network [1..1] IEEE8021X TlsVerify

Verification of the server-side certificate of an IEEE802.1x connection against the certificates in the local CA-list when TLS is used. The CA-list must be uploaded to the video system / codec.

This setting takes effect only when Network [1..1] IEEE8021X Eap Tls is enabled (On).

Requires user role: ADMIN

Value space: `<Off/On>`

Off: When set to Off, TLS connections are allowed without verifying the server-side X.509 certificate against the local CA-list. This should typically be selected if no CA-list has been uploaded to the codec.
On: When set to On, the server-side X.509 certificate will be validated against the local CA-list for all TLS connections. Only servers with a valid certificate will be allowed.

Example: `xConfiguration Network 1 IEEE8021X TlsVerify: Off`

Network [1..1] IEEE8021X UseClientCertificate

Authentication using a private key/certificate pair during an IEEE802.1x connection. The authentication X.509 certificate must be uploaded to the video system / codec.

Requires user role: ADMIN

Value space: `<Off/On>`

Off: When set to Off client-side authentication is not used (only server-side).
On: When set to On the client (codec) will perform a mutual authentication TLS handshake with the server.

Example: `Network 1 IEEE8021X UseClientCertificate: Off`

Network [1..1] IEEE8021X Identity

The 802.1X Identity is the user name needed for 802.1X authentication.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: String with a maximum of 64 characters.

Example: `Network 1 IEEE8021X Identity: ""`

Network [1..1] IEEE8021X Password

The 802.1X Password is the password needed for 802.1X authentication.

Requires user role: ADMIN

Value space: `<S: 0, 32>`

Format: String with a maximum of 32 characters.

Example: `Network 1 IEEE8021X Password: "***"`

Network [1..1] IEEE8021X AnonymousIdentity

The 802.1X Anonymous ID string is to be used as unencrypted identity with EAP (Extensible Authentication Protocol) types that support different tunneled identity, like EAP-PEAP and EAP-TTLS. If set, the anonymous ID will be used for the initial (unencrypted) EAP Identity Request.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: String with a maximum of 64 characters.

Example: `Network 1 IEEE8021X AnonymousIdentity: ""`

Network [1..1] IEEE8021X Eap Md5

Set the Md5 (Message-Digest Algorithm 5) mode. This is a Challenge Handshake Authentication Protocol that relies on a shared secret. Md5 is a Weak security.

Requires user role: ADMIN

Value space: `<On/Off>`

On: The EAP-MD5 protocol is enabled (default).
Off: The EAP-MD5 protocol is disabled.

Example: `Network 1 IEEE8021X Eap Md5: On`

Network [1..1] IEEE8021X Eap Ttls

Set the TTLS (Tunneled Transport Layer Security) mode. Authenticates LAN clients without the need for client certificates. Developed by Funk Software and Certicom. Usually supported by Agere Systems, Proxim and Avaya.

Requires user role: ADMIN

Value space: `<On/Off>`

On: The EAP-TTLS protocol is enabled (default).
Off: The EAP-TTLS protocol is disabled.

Example: `Network 1 IEEE8021X Eap Ttls: On`

Network [1..1] IEEE8021X Eap Tls

Enable or disable the use of EAP-TLS (Transport Layer Security) for IEEE802.1x connections. The EAP-TLS protocol, defined in RFC5216, is considered one of the most secure EAP standards. LAN clients are authenticated using client certificates.

Requires user role: ADMIN

Value space: `<Off/On>`

Off: The EAP-TLS protocol is disabled.
On: The EAP-TLS protocol is enabled (default).

Example: `Network 1 IEEE8021X Eap Tls: On`

Network [1..1] IEEE8021X Eap Peap

Set the Peap (Protected Extensible Authentication Protocol) mode. Authenticates LAN clients without the need for client certificates. Developed by Microsoft, Cisco and RSA Security.

Requires user role: ADMIN

Value space: `<On/Off>`

On: The EAP-PEAP protocol is enabled (default).
Off: The EAP-PEAP protocol is disabled.

Example: `Network 1 IEEE8021X Eap Peap: On`

Network [1..1] MTU

Set the Ethernet MTU (Maximum Transmission Unit).

Requires user role: ADMIN

Value space: `<576..1500>`

Range: Select a value from 576 to 1500 bytes.

Example: `Network 1 MTU: 1500`

Network [1..1] Speed

Set the Ethernet link speed.

Requires user role: ADMIN

Value space: `<Auto/10half/10full/100half/100full/1000full>`

Auto: Autonegotiate link speed.
10half: Force link to 10 Mbps half-duplex.
10full: Force link to 10 Mbps full-duplex.
100half: Force link to 100 Mbps half-duplex.
100full: Force link to 100 Mbps full-duplex.
1000full: Force link to 1 Gbps full-duplex.

Example: `Network 1 Speed: Auto`

Network [1..1] TrafficControl Mode

Set the network traffic control mode to decide how to control the video packets transmission speed.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Transmit video packets at maximum 20 Mbps. Can be used to smooth out bursts in the outgoing network traffic.
Off: Transmit video packets at link speed.

Example: `Network 1 TrafficControl: On`

Network [1..1] RemoteAccess Allow

Filter IP addresses for access to ssh/telnet/HTTP/HTTPS.

Requires user role: ADMIN

Value space: `<S: 0, 255>`

Format: String with a maximum of 255 characters, comma separated IP adresses or IP range.

Example: `Network 1 RemoteAccess Allow: "192.168.1.231, 192.168.1.182"`

Network [1..1] VLAN Voice Mode

Set the VLAN voice mode.

Requires user role: ADMIN

Value space: `<Auto/Manual/Off>`

Auto: The Cisco Discovery Protocol (CDP), if available, assigns an id to the voice VLAN. If CDP is not available, VLAN is not enabled. The VLAN Voice Mode automatically will be set to Auto when the GUI is used to set the Provisioning Mode to CUCM.

Manual: The VLAN id is set manually using the Network VLAN Voice VlanId setting. If CDP is available, the manually set value will be overruled by the value assigned by CDP.

Off: VLAN is not enabled.

Example: `Network 1 VLAN Voice Mode: Off`

Network [1..1] VLAN Voice VlanId

Set the VLAN voice ID. This setting will only take effect if VLAN Voice Mode is set to Manual.

Requires user role: ADMIN

Value space: `<1..4094>`

Range: Select a value from 1 to 4094.

Example: `Network 1 VLAN Voice VlanId: 1`

The NetworkServices settings

NetworkServices MultiWay Address

The Multiway address must be equal to the Conference Factory Alias, as configured on the Video Communication Server. The Multiway™ conferencing enables video endpoint users to introduce a 3rd party into an existing call.

Multiway™ can be used in the following situations:

1) When you want to add someone else in to your existing call.

2) When you are called by a 3rd party while already in a call and you want to include that person in the call.

Requirements: The Codec C20 must be running TC3.0 (or later), Codec C90/C60/C40 must be running TC4.0 (or later), EX90/EX60/MX200 must be running TC4.2 (or later), MX300 must be running TC5.0 (or later),Video Communication Server (VCS) version X5 (or later) and Codian MCU version 3.1 (or later). Endpoints invited to join the Multiway™ conference must support the H.323 routeToMC facility message if in an H.323 call, or SIP REFER message if in a SIP call.

Requires user role: ADMIN

Value space: `<S: 0, 255>`

Format: String with a maximum of 255 characters.

Example: `NetworkServices MultiWay Address: "h323:multiway@company.com"`

NetworkServices MultiWay Protocol

Determine the protocol to be used for Multiway calls. NOTE: Requires a restart of the codec.

Requires user role: ADMIN

Value space: `<Auto/H323/Sip>`

Auto: The system will select the protocol for Multiway calls.
H323: The H323 protocol will be used for Multiway calls.
Sip: The SIP protocol will be used for Multiway calls.

Example: `NetworkServices MultiWay Protocol: Auto`

NetworkServices H323 Mode

Determine whether the system should be able to place and receive H.323 calls or not. NOTE: Requires a restart of the codec.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable the possibility to place and receive H.323 calls (default).
Off: Disable the possibility to place and receive H.323 calls.

Example: `NetworkServices H323 Mode: On`

NetworkServices HTTP Mode

Set the HTTP mode to enable/disable access to the system through a web browser. The web interface is used for system management, call management such as call transfer, diagnostics and software uploads.

Requires user role: ADMIN

Value space: `<On/Off>`

On: The HTTP protocol is enabled.
Off: The HTTP protocol is disabled.

Example: `NetworkServices HTTP Mode: On`

NetworkServices HTTPS Mode

HTTPS is a web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the web server.

Requires user role: ADMIN

Value space: `<On/Off>`

On: The HTTPS protocol is enabled.
Off: The HTTPS protocol is disabled.

Example: `NetworkServices HTTPS Mode: On`

NetworkServices HTTPS VerifyServerCertificate

When the system connects to an external HTTPS server (like a phonebook server or an external manager), this server will present a certificate to the system to identify itself.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Requires the system to verify that the server certificate is signed by a trusted Certificate Authority (CA). This requires that a list of trusted CAs are uploaded to the system in advance.
Off: Do not verify server certificates.

Example: `NetworkServices HTTPS VerifyServerCertificate: Off`

NetworkServices HTTPS VerifyClientCertificate

When the system connects to a HTTPS client (like a web browser), the client can be asked to present a certificate to the system to identify itself.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Requires the client to present a certificate that is signed by a trusted Certificate Authority (CA). This requires that a list of trusted CAs are uploaded to the system in advance.
Off: Do not verify client certificates.

Example: `NetworkServices HTTPS VerifyClientCertificate: Off`

NetworkServices HTTPS OCSP Mode

Define the support for OCSP (Online Certificate Status Protocol) responder services. The OCSP feature allows users to enable OCSP instead of certificate revocation lists (CRLs) to check certificate status.

Requires user role: ADMIN

Value space: `<Off/On>`

Off: Disable OCSP support.
On: Enable OCSP support.

Example: `NetworkServices HTTPS OCSP Mode: Off`

NetworkServices HTTPS OCSP URL

Specify the URL of an OCSP server.

Requires user role: ADMIN

Value space: `<S: 0, 255>`

Format: String with a maximum of 255 characters.

Example: `NetworkServices HTTPS OCSP URL: "http://ocspserver.company.com:81"`

NetworkServices NTP Mode

The Network Time Protocol (NTP) is used to synchronize the time of the system to a reference time server. The time server will subsequently be queried every 24th hour for time updates. The time will be displayed on the top of the screen. The system will use the time to timestamp messages transmitted to Gatekeepers or Border Controllers requiring H.235 authentication. The system will use the time to timestamp messages transmitted to Gatekeepers or Border Controllers that requires H.235 authentication. It is also used for timestamping Placed Calls, Missed Calls and Received Calls.

Requires user role: ADMIN

Value space: `<Off/Auto/Manual>`

Off: The system will not use an NTP server.
Auto: The system will use the NTP server, by which address is supplied from the DHCP server in the network. If no DHCP server is used, or the DHCP server does not provide the system with a NTP server address, the system will use the static defined NTP server address specified by the user.
Manual: The system will always use the static defined NTP server address specified by the user.

Example: `NetworkServices NTP Mode: Manual`

NetworkServices NTP Address

Enter the NTP Address to define the network time protocol server address. This address will be used if NTP Mode is set to Manual, or if set to Auto and no address is supplied by a DHCP server.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: String with a maximum of 64 characters.

Example: `NetworkServices NTP Address: "1.ntp.tandberg.com"`

NetworkServices SIP Mode

Determine whether the system should be able to place and receive SIP calls or not. NOTE: Requires a restart of the codec.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable the possibility to place and receive SIP calls (default).
Off: Disable the possibility to place and receive SIP calls.

Example: `NetworkServices SIP Mode: On`

NetworkServices SNMP Mode

SNMP (Simple Network Management Protocol) is used in network management systems to monitor network-attached devices (routers, servers, switches, projectors, etc) for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (set to ReadOnly) and sometimes set (set to ReadWrite) by managing applications.

Requires user role: ADMIN

Value space: `<Off/ReadOnly/ReadWrite>`

Off: Disable the SNMP network service.
ReadOnly: Enable the SNMP network service for queries only.
ReadWrite: Enable the SNMP network service for both queries and commands.

Example: `NetworkServices SNMP Mode: ReadWrite`

NetworkServices SNMP Host [1..3] Address

Enter the address of up to three SNMP Managers.

The system's SNMP Agent (in the codec) responds to requests from SNMP Managers (a PC program etc.), e.g. about system location and system contact. SNMP traps are not supported.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: String with a maximum of 64 characters.

Example: `NetworkServices SNMP Host 1 Address: ""`

NetworkServices SNMP CommunityName

Enter the name of the Network Services SNMP Community. SNMP Community names are used to authenticate SNMP requests. SNMP requests must have a password (case sensitive) in order to receive a response from the SNMP Agent in the codec. The default password is " public". If you have the Cisco TelePresence Management Suite (TMS) you must make sure the same SNMP Community is configured there too. NOTE: The SNMP Community password is case sensitive.

Requires user role: ADMIN

Value space: `<S: 0, 50>`

Format: String with a maximum of 50 characters.

Example: `NetworkServices SNMP CommunityName: "public"`

NetworkServices SNMP SystemContact

Enter the name of the Network Services SNMP System Contact.

Requires user role: ADMIN

Value space: `<S: 0, 50>`

Format: String with a maximum of 50 characters.

Example: `NetworkServices SNMP SystemContact: ""`

NetworkServices SNMP SystemLocation

Enter the name of the Network Services SNMP System Location.

Requires user role: ADMIN

Value space: `<S: 0, 50>`

Format: String with a maximum of 50 characters.

Example: `NetworkServices SNMP SystemLocation: ""`

NetworkServices SSH Mode

SSH (or Secure Shell) protocol can provide secure encrypted communication between the codec and your local computer.

Requires user role: ADMIN

Value space: `<On/Off>`

On: The SSH protocol is enabled.

Off: The SSH protocol is disabled.

Example: `NetworkServices SSH Mode: On`

NetworkServices SSH AllowPublicKey

Secure Shell (SSH) public key authentication can be used to access the codec.

Requires user role: ADMIN

Value space: `<On/Off>`

On: The SSH public key is allowed.

Off: The SSH public key is not allowed.

Example: `NetworkServices SSH AllowPublicKey: On`

NetworkServices Telnet Mode

Telnet is a network protocol used on the Internet or Local Area Network (LAN) connections.

Requires user role: ADMIN

Value space: `<On/Off>`

On: The Telnet protocol is enabled.

Off: The Telnet protocol is disabled. This is the factory setting.

Example: `NetworkServices Telnet Mode: Off`

The Phonebook settings

Phonebook Server [1..1] ID

Enter a name for the external phonebook.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: String with a maximum of 64 characters.

Example: `Phonebook Server 1 ID: ""`

Phonebook Server [1..1] Type

Select the phonebook server type.

Requires user role: ADMIN

Value space: `<VCS/TMS/Callway/CUCM>`

VCS: Select VCS if the phonebook is located on the Cisco TelePresence Video Communication Server.
TMS: Select TMS if the phonebook is located on the Cisco TelePresence Management Suite server.
Callway: Select Callway if the phonebook is to be provided by the Callway subscription service. Contact your Callway provider for more information.
CUCM: Select CUCM if the phonebook is located on the Cisco Unified Communications Manager.

Example: `Phonebook Server 1 Type: TMS`

Phonebook Server [1..1] URL

Enter the address (URL) to the external phonebook server.

Requires user role: ADMIN

Value space: `<S: 0, 255>`

Format: String with a maximum of 255 characters.

Example: `Phonebook Server 1 URL: "http://tms.company.com/tms/public/external/phonebook/phonebookservice.asmx"`

The Provisioning settings

Provisioning Connectivity

This setting controls how the device discovers whether it should request an internal or external configuration from the provisioning server.

Requires user role: ADMIN

Value space: `<Internal/External/Auto>`

Internal: Request internal configuration.
External: Request external configuration.
Auto: Automatically discover using NAPTR queries whether internal or external configurations should be requested. If the NAPTR responses have the " e" flag, external configurations will be requested. Otherwise internal configurations will be requested.

Example: `Provisioning Connectivity: Auto`

Provisioning Mode

It is possible to configure the codec (video system) using a provisioning system / an external manager. This allows video conferencing network administrators to manage many video systems simultaneously.

With this setting you choose which type of provisioning system to use. Provisioning can also be switched off. Contact your provisioning system provider/representative for more information.

Requires user role: ADMIN

Value space: `<Off/TMS/VCS/CallWay/CUCM/Auto>`

Off: The video system will not be configured by a provisioning system.
TMS: The video system will be configured using TMS (Cisco TelePresence Management System).
VCS: The video system will be configured using VCS (Cisco TelePresence Video Communication Server).
Callway: The video system will be configured using Callway (subscription service).
CUCM: The video system will be configured using CUCM (Cisco Unified Communications Manager).
Auto: The provisioning server will automatically be selected by the video system.

Example: `Provisioning Mode: TMS`

Provisioning LoginName

This is the user name part of the credentials used to authenticate the video system with the provisioning server. This setting must be used when required by the provisioning server. If Provisioning Mode is Callway, enter the video number.

Requires user role: ADMIN

Value space: `<S: 0, 80>`

Format: String with a maximum of 80 characters.

Example: `Provisioning LoginName: ""`

Provisioning Password

This is the password part of the credentials used to authenticate the video system with the provisioning server. This setting must be used when required by the provisioning server. If Provisioning Mode is Callway, enter the activation code.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: String with a maximum of 64 characters.

Example: `Provisioning Password: ""`

Provisioning HttpMethod

Select the HTTP method to be used for the provisioning.

Requires user role: ADMIN

Value space: `<GET/POST>`

GET: Select GET when the provisiong server supports GET.
POST: Select POST when the provisiong server supports POST.

Example: `Provisioning HttpMethod: POST`

Provisioning ExternalManager Address

Enter the IP Address or DNS name of the external manager / provisioning system.

If an External Manager Address (and Path) is configured, the system will send a message to this address when starting up. When receiving this message the external manager / provisioning system can return configurations/commands to the unit as a result.

When using CUCM or TMS provisioning, the DHCP server can be set up to provide the external manager address automatically (DHCP Option 242 for TMS, and DHCP Option 150 for CUCM). An address set in the Provisioning ExternalManager Address setting will override the address provided by DHCP.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: A valid IP address format or DNS name; a compact string with a maximum of 64 characters.

Example: `Provisioning ExternalManager Address: ""`

Provisioning ExternalManager Protocol

Determine whether to use secure management or not.

Requires user role: ADMIN

Value space: `<HTTP/HTTPS>`

HTTP: Set to HTTP to disable secure management. Requires HTTP to be enabled in the xConfiguration NetworkServices HTTP Mode setting.

HTTPS: Set to HTTPS to enable secure management. Requires HTTPS to be enabled in the xConfiguration NetworkServices HTTPS Mode setting.

Example: `Provisioning ExternalManager Protocol: HTTP`

Provisioning ExternalManager Path

Set the Path to the external manager / provisioning system. This setting is required when several management services reside on the same server, i.e. share the same External Manager address.

Requires user role: ADMIN

Value space: `<S: 0, 255>`

Format: String with a maximum of 255 characters.

Example: `Provisioning ExternalManager Path: "tms/public/external/management/SystemManagementService.asmx"`

Provisioning ExternalManager Domain

Enter the SIP domain for the VCS provisioning server.

Requires user role: ADMIN

Value space: `<S: 0, 64>`

Format: String with a maximum of 64 characters.

Example: `Provisioning ExternalManager Domain: "any.domain.com"`

The RTP settings

RTP Ports Range Start

Specify the first port in the range of RTP ports. See also the " H323 Profile [1..1] PortAllocation" command.

Requires user role: USER

Value space: `<1024..65502>`

Range: Select a value from 1024 to 65502.

Example: `RTP Ports Range Start: 2326`

RTP Ports Range Stop

Specify the last RTP port in the range. See also the " H323 Profile [1..1] PortAllocation" command.

Requires user role: USER

Value space: `<1056..65535>`

Range: Select a value from 1056 to 65535.

Example: `RTP Ports Range Stop: 2486`

The Security settings

Security Audit Server Address

Enter the external/global IP-address to the audit syslog server. IPv6 is not supported.

NOTE: Requires a restart of the system for any change to take effect.

Requires user role: AUDIT

Value space: `<S: 0, 64>`

Format: String with a maximum of 64 characters.

Example: `Security Audit Server Address: ""`

Security Audit Server Port

Enter the port of the syslog server that the system shall send its audit logs to. The default port is 514.

NOTE: Requires a restart of the system for any change to take effect.

Requires user role: AUDIT

Value space: `<0..65535>`

Range: Select a value from 0 to 65535.

Example: `Security Audit Server Port: 514`

Security Audit OnError Action

Describes what actions will be taken if connection to the syslog server is lost. This setting is only relevant if Security Audit Logging Mode is set to ExternalSecure.

NOTE: Requires a restart of the system for any change to take effect.

Requires user role: AUDIT

Value space: `<Halt/Ignore>`

Halt: If a halt condition is detected the unit is rebooted and only the auditor is allowed to operate the unit until the halt condition has passed. When the halt condition has passed the audit logs are re-spooled to the external server. Halt conditions are: A network breach (no physical link), no external syslog server running (or wrong server address or port), TLS authentication failed (if in use), local backup (re-spooling) log full.

Ignore: The system will continue its normal operation, and rotate internal logs when full. When connection is restored it will again send its audit logs to the syslog server.

Example: `Security Audit OnError Action: Ignore`

Security Audit Logging Mode

Describes where the audit logs are recorded or transmitted.

NOTE: Requires a restart of the system for any change to take effect.

Requires user role: AUDIT

Value space: `<Off/Internal/External/ExternalSecure>`

Off: No audit logging is performed.

Internal: The system records the audit logs to internal logs, and rotates logs when they are full.

External: The system sends the audit logs to an external audit syslog server. The external server must support TCP.

ExternalSecure: The system sends encrypted audit logs to an external audit server that is verified by a certificate in the Audit CA list. The Audit CA list file must be uploaded to the codec using the web interface. The common_name parameter of a certificate in the CA list must match the IP address of the syslog server.

Example: `Security Audit Logging Mode: Off`

Security Session ShowLastLogon

When logging in to the system using SSH or Telnet you will see the UserId, time and date of the last session that did a successful login.

Requires user role: ADMIN

Value space: `<Off/On>`

On: Set to On to enable the possibility to show information about the last session.

Off: Set to Off to disable the possibility to show information about the last session.

Example: `Security Session ShowLastLogon: Off`

Security Session InactivityTimeout

Determines how long the system will accept inactivity from the user before he is automatically logged out.

Requires user role: ADMIN

Value space: `<0..10000>`

Range: Select a value from 0 to 10000 seconds. 0 means that inactivity will not enforce automatically logout.

Example: `Security Session InactivityTimeout: 0`

The SerialPort settings

SerialPort Mode

Set the COM 1 serial port to be enabled/disabled.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable the COM 1 serial port.
Off: Disable the COM 1 serial port.

Example: `SerialPort Mode: On`

SerialPort BaudRate

Specify the baud rate (data transmission rate, bits per second) for the COM 1 port. The default value is 38400.

Connection parameters for the COM port: Data bits: 8; Parity: None; Stop bits: 1; Flow control: None.

Requires user role: ADMIN

Value space: `<9600/19200/38400/57600/115200>`

Range: Select a baud rate from the baud rates listed (bps).

Example: `SerialPort BaudRate: 38400`

SerialPort LoginRequired

Determine if login shall be required when connecting to the COM 1 port.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Login is required when connecting to the codec through COM 1 port.
Off: The user can access the codec through COM 1 port without any login.

Example: `SerialPort LoginRequired: On`

The SIP settings

SIP Profile [1..1] URI

The SIP URI or number is used to address the system. This is the URI that is registered and used by the SIP services to route inbound calls to the system. A Uniform Resource Identifier (URI) is a compact string of characters used to identify or name a resource.

Requires user role: ADMIN

Value space: `<S: 0, 255>`

Format: Compact string with a maximum of 255 characters.

Example: `SIP Profile 1 URI: "sip:firstname.lastname@company.com"`

SIP Profile [1..1] DisplayName

When configured the incoming call will report the DisplayName instead of the SIP URI.

Requires user role: ADMIN

Value space: `<S: 0, 255>`

Format: String with a maximum of 255 characters.

Example: `SIP Profile 1 DisplayName: ""`

SIP Profile [1..1] Authentication [1..1] LoginName

This is the user name part of the credentials used to authenticate towards the SIP proxy.

Requires user role: ADMIN

Value space: `<S: 0, 128>`

Format: String with a maximum of 128 characters.

Example: `SIP Profile 1 Authentication 1 LoginName: ""`

SIP Profile [1..1] Authentication [1..1] Password

This is the password part of the credentials used to authenticate towards the SIP proxy.

Requires user role: ADMIN

Value space: `<S: 0, 128>`

Format: String with a maximum of 128 characters.

Example: `SIP Profile 1 Authentication 1 Password:`

SIP Profile [1..1] DefaultTransport

Select the transport protocol to be used over the LAN.

Requires user role: ADMIN

Value space: `<UDP/TCP/Tls/Auto>`

UDP: The system will always use UDP as the default transport method.

TCP: The system will always use TCP as the default transport method.

Tls: The system will always use TLS as the default transport method. For TLS connections a SIP CA-list can be uploaded to the video system. If no such CA-list is available on the system then anonymous Diffie Hellman will be used.

Auto: The system will try to connect using transport protocols in the following order: TLS, TCP, UDP.

Example: `SIP Profile 1 DefaultTransport: Auto`

SIP Profile [1..1] TlsVerify

For TLS connections a SIP CA-list can be uploaded to the video system.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Set to On to verify TLS connections. Only TLS connections to servers, whose x.509 certificate is validated against the CA-list, will be allowed.

Off: Set to Off to allow TLS connections without verifying them. The TLS connections are allowed to be set up without verifying the x.509 certificate received from the server against the local CA-list. This should typically be selected if no SIP CA-list has been uploaded.

Example: `SIP Profile 1 TlsVerify: Off`

SIP Profile [1..1] Outbound

The client initiated connections mechanism for firewall traversal, connection reuse and redundancy. The current version supports http://tools.ietf.org/html/draft-ietf-sip-outbound-20.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Set up multiple outbound connections to servers in the Proxy Address list.

Off: Connect to the single proxy configured first in Proxy Address list.

Example: `SIP Profile 1 Outbound: Off`

SIP Profile [1..1] Proxy [1..4] Address

The Proxy Address is the manually configured address for the outbound proxy. It is possible to use a fully qualified domain name, or an IP address. The default port is 5060 for TCP and UDP but another one can be provided. If Outbound is enabled, multiple proxies can be addressed.

Requires user role: ADMIN

Value space: `<S: 0, 255>`

Format: Compact string with a maximum of 255 characters. An IP address that contains letters (192.a.2.0) or unvalid IP addresses (192.0.1234.0) will be rejected.

Example: `SIP Profile 1 Proxy 1 Address: ""`

SIP Profile [1..1] Proxy [1..4] Discovery

Select if the SIP Proxy address is to be obtained manually or by using Dynamic Host Configuration Protocol (DHCP).

Requires user role: ADMIN

Value space: `<Auto/Manual>`

Auto: When Auto is selected, the SIP Proxy address is obtained using Dynamic Host Configuration Protocol (DHCP).

Manual: When Manual is selected, the manually configured SIP Proxy address will be used.

Example: `SIP Profile 1 Proxy 1 Discovery: Manual`

SIP Profile [1..1] Type

Enables SIP extensions and special behaviour for a vendor or provider.

Requires user role: ADMIN

Value space: `<Standard/Alcatel/Avaya/Cisco/Microsoft/Nortel>`

Standard: To be used when registering to standard SIP Proxy (tested with Cisco TelePresence VCS and Broadsoft)

Alcatel: To be used when registering to Alcatel-Lucent OmniPCX Enterprise. NOTE: This mode is not fully supported.

Avaya: To be used when registering to Avaya Communication Manager. NOTE: This mode is not fully supported.

Cisco: To be used when registering to Cisco Unified Communication Manager.

Microsoft: To be used when registering to Microsoft LCS or OCS. NOTE: This mode is not fully supported.

Nortel: To be used when registering to Nortel MCS 5100 or MCS 5200 PBX. NOTE: This mode is not fully supported.

Example: `SIP Profile 1 Type: Standard`

The Standby settings

Standby Control

Determine whether the system should go into standby mode or not.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enter standby mode when the Standby Delay has timed out. NOTE: Requires the Standby Delay to be set to an appropriate value.
Off: The system will not enter standby mode.

Example: `Standby Control: On`

Standby Delay

Define how long (in minutes) the system shall be in idle mode before it goes into standby mode. NOTE: Requires the Standby Control to be enabled.

Requires user role: ADMIN

Value space: `<1..480>`

Range: Select a value from 1 to 480 minutes.

Example: `Standby Delay: 10`

Standby BootAction

Define the camera position after a restart of the codec.

Requires user role: ADMIN

Value space: `<None/Preset1/Preset2/Preset3/Preset4/Preset5/Preset6/Preset7/Preset8/Preset9/Preset10/Preset11/Preset12/Preset13/Preset14/Preset15/RestoreCameraPosition/DefaultCameraPosition>`

None: No action.
Preset1 to Preset15: After a reboot the camera position will be set to the position defined by the selected preset.
RestoreCameraPosition: After a reboot the camera position will be set to the position it had before the last boot.
DefaultCameraPosition: After a reboot the camera position will be set to the factory default position.

Example: `Standby BootAction: DefaultCameraPosition`

Standby StandbyAction

Define the camera position when going into standby mode.

Requires user role: ADMIN

Value space: `<None/PrivacyPosition>`

None: No action.
PrivacyPosition: Turns the camera to a sideways position for privacy.

Example: `Standby StandbyAction: PrivacyPosition`

Standby WakeupAction

Define the camera position when leaving standby mode.

Requires user role: ADMIN

Value space: `<None/Preset1/Preset2/Preset3/Preset4/Preset5/Preset6/Preset7/Preset8/Preset9/Preset10/Preset11/Preset12/Preset13/Preset14/Preset15/RestoreCameraPosition/DefaultCameraPosition>`

None: No action.
Preset1 to Preset15: When leaving standby the camera position will be set to the position defined by the selected preset.
RestoreCameraPosition: When leaving standby the camera position will be set to the position it had before entering standby.
DefaultCameraPosition: When leaving standby the camera position will be set to the factory default position.

Example: `Standby WakeupAction: RestoreCameraPosition`

The SystemUnit settings

SystemUnit Name

Enter a System Name to define a name of the system unit. If the H.323 Alias ID is configured on the system then this ID will be used instead of the system name. The system name will be displayed:

1) When the codec is acting as an SNMP Agent.

2) Towards a DHCP server.

Requires user role: ADMIN

Value space: `<S: 0, 50>`

Format: String with a maximum of 50 characters.

Example: `SystemUnit Name: "Meeting Room"`

SystemUnit MenuLanguage

Select the language to be used in the menus on screen.

Requires user role: USER

Value space: `<English/ChineseSimplified/ChineseTraditional/Czech/Danish/Dutch/Finnish/French/German/Hungarian/Italian/Japanese/Korean/Norwegian/Polish/PortugueseBrazilian/Russian/Spanish/SpanishLatin/Swedish/Turkish>`

Example: `SystemUnit MenuLanguage: English`

SystemUnit ContactInfo Type

Describes which parameter to put in the status field in the upper left corner on the screen display. The information can also be read with the command xStatus SystemUnit ContactInfo.

Requires user role: ADMIN

Value space: `<Auto/None/IPv4/IPv6/H323Id/E164Alias/SipUri/SystemName>`

Auto: Shows the address which another system can dial to reach this system, depending on the default call protocol and system registration.
None: Do not show any contact information.
IPv4: Shows the IPv4 address as the contact information.
IPv6: Shows the IPv6 address as the contact information.
H323Id: Shows the H323 ID as the contact information.
E164Alias: Shows the H323 E164 Alias as the contact information.
SipUri: Shows the SIP URI as the contact information.
SystemName: Shows the system name as the contact information.

Example: `SystemUnit ContactInfo Type: Auto`

SystemUnit CallLogging Mode

Set the call logging mode for calls that are received or placed by the system. The call logs may then be viewed via the web interface or using the xHistory command.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable logging.
Off: Disable logging.

Example: `SystemUnit CallLogging Mode: On`

SystemUnit IrSensor

Both the Codec C Series and PrecisionHD camera have IR sensors, and only one of them needs to be enabled at the time. The IR sensor LED is located on the front of the codec and the camera and flickers when an IR signal is received from the remote control.

Requires user role: ADMIN

Value space: `<On/Off/Auto>`

On: Enable the IR sensor on the codec.
Off: Disable the IR sensor on the codec.
Auto: The system will automatically disable the IR sensor on the codec if the IR sensor at camera is enabled. Otherwise, the IR sensor on the codec will be enabled.

Example: `SystemUnit IrSensor: Auto`

The Time settings

Time Zone

Set the time zone where the system is located, using Windows time zone description format.

Requires user role: USER

Value space: `<GMT-12:00 (International Date Line West)/GMT-11:00 (Midway Island, Samoa)/GMT-10:00 (Hawaii)/GMT-09:00 (Alaska)/GMT-08:00 (Pacific Time (US & Canada); Tijuana)/GMT-07:00 (Arizona)/GMT-07:00 (Mountain Time (US & Canada))/GMT-07:00 (Chihuahua, La Paz, Mazatlan)/GMT-06:00 (Central America)/GMT-06:00 (Saskatchewan)/GMT-06:00 (Guadalajara, Mexico City, Monterrey)/GMT-06:00 (Central Time (US & Canada))/GMT-05:00 (Indiana (East))/GMT-05:00 (Bogota, Lima, Quito)/GMT-05:00 (Eastern Time (US & Canada))/GMT-04:30 (Caracas)/GMT-04:00 (La Paz)/GMT-04:00 (Santiago)/GMT-04:00 (Atlantic Time (Canada))/GMT-03:30 (Newfoundland)/GMT-03:00 (Buenos Aires, Georgetown)/GMT-03:00 (Greenland)/GMT-03:00 (Brasilia)/GMT-02:00 (Mid-Atlantic)/GMT-01:00 (Cape Verde Is.)/GMT-01:00 (Azores)/GMT (Casablanca, Monrovia)/GMT (Coordinated Universal Time)/GMT (Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London)/GMT+01:00 (West Central Africa)/GMT+01:00 (Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna)/GMT+01:00 (Brussels, Copenhagen, Madrid, Paris)/GMT+01:00 (Sarajevo, Skopje, Warsaw, Zagreb)/GMT+01:00 (Belgrade, Bratislava, Budapest, Ljubljana, Prague)/GMT+02:00 (Harare, Pretoria)/GMT+02:00 (Jerusalem)/GMT+02:00 (Athens, Istanbul, Minsk)/GMT+02:00 (Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius)/GMT+02:00 (Cairo)/GMT+02:00 (Bucharest)/GMT+03:00 (Nairobi)/GMT+03:00 (Kuwait, Riyadh)/GMT+03:00 (Moscow, St. Petersburg, Volgograd)/GMT+03:00 (Baghdad)/GMT+03:30 (Tehran)/GMT+04:00 (Abu Dhabi, Muscat)/GMT+04:00 (Baku, Tbilisi, Yerevan)/GMT+04:30 (Kabul)/GMT+05:00 (Islamabad, Karachi, Tashkent)/GMT+05:00 (Ekaterinburg)/GMT+05:30 (Chennai, Kolkata, Mumbai, New Delhi)/GMT+05:45 (Kathmandu)/GMT+06:00 (Sri Jayawardenepura)/GMT+06:00 (Astana, Dhaka)/GMT+06:00 (Almaty, Novosibirsk)/GMT+06:30 (Rangoon)/GMT+07:00 (Bangkok, Hanoi, Jakarta)/GMT+07:00 (Krasnoyarsk)/GMT+08:00 (Perth)/GMT+08:00 (Taipei)/GMT+08:00 (Kuala Lumpur, Singapore)/GMT+08:00 (Beijing, Chongqing, Hong Kong, Urumqi)/GMT+08:00 (Irkutsk, Ulaan Bataar)/GMT+09:00 (Osaka, Sapporo, Tokyo)/GMT+09:00 (Seoul)/GMT+09:00 (Yakutsk)/GMT+09:30 (Darwin)/GMT+09:30 (Adelaide)/GMT+10:00 (Guam, Port Moresby)/GMT+10:00 (Brisbane)/GMT+10:00 (Vladivostok)/GMT+10:00 (Hobart)/GMT+10:00 (Canberra, Melbourne, Sydney)/GMT+11:00 (Magadan, Solomon Is., New Caledonia)/GMT+12:00 (Fiji, Kamchatka, Marshall Is.)/GMT+12:00 (Auckland, Wellington)/GMT+13:00 (Nuku alofa)>`

Range: Select a time zone from the list time zones. If using a command line interface; watch up for typos.

Example: `Time Zone: "GMT (Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London)"`

Time TimeFormat

Set the time format.

Requires user role: USER

Value space: `<24H/12H>`

24H: Set the time format to 24 hours.

12H: Set the time format to 12 hours (AM/PM).

Example: `Time TimeFormat: 24H`

Time DateFormat

Set the date format.

Requires user role: USER

Value space: `<DD_MM_YY/MM_DD_YY/YY_MM_DD>`

DD_MM_YY: The date January 30th 2010 will be displayed: 30.01.10

MM_DD_YY: The date January 30th 2010 will be displayed: 01.30.10

YY_MM_DD: The date January 30th 2010 will be displayed: 10.01.30

Example: `Time DateFormat: DD_MM_YY`

The UserInterface settings

UserInterface TouchPanel DefaultPanel

Select whether to display the list of contacts or the list of scheduled meetings on the Touch panel as default.

Requires user role: USER

Value space: `<ContactList/MeetingList>`

ContactList: The contact list (favorites, directory and history) will appear as default on the Touch panel.

MeetingList: The list of scheduled meetings will appear as default on the Touch panel.

Example: `UserInterface TouchPanel DefaultPanel: ContactList`

The Video settings

Video Input Source [1..2] Name

Enter a name for the video input source.

Requires user role: ADMIN

Value space: `<S: 0, 50>`

Format: String with a maximum of 50 characters.

Example: `Video Input Source 1 Name: ""`

Video Input Source [1] Connector

Select which video input connector to be active on video input source 1.

Requires user role: ADMIN

Value space: `<HDMI>`

HDMI: Select HDMI when you want to use the HDMI as input source 1.

Example: `Video Input Source 1 Connector: HDMI`

Video Input Source [2] Connector

Select which video input connector to be active on video input source 2.

Requires user role: ADMIN

Value space: `<DVI>`

DVI: Select DVI-I when you want to use the DVI-I 2 as input source 2.

Example: `Video Input Source 2 Connector: DVI`

Video Input Source [1..2] Type

Set which type of input source is connected to the video input.

Requires user role: ADMIN

Value space: `<other/camera/PC/DVD/document_camera>`

Other: Select Other when some other type of equipment is connected to the selected video input.
Camera: Select Camera when you have a camera connected to the selected video input.
PC: Select PC when you have a PC connected to the selected video input.
DVD: Select DVD when you have a DVD player connected to the selected video input.
Document_Camera: Select Document_Camera when you have a document camera connected to the selected video input.

Example: `Video Input Source 1 Type: PC`

Video Input Source [1..2] CameraControl Mode

Select whether or not to enable camera control for the selected video input source when the video input is active.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable camera control.
Off: Disable camera control.

Example: `Video Input Source 1 CameraControl Mode: On`

Video Input Source [1..2] CameraControl CameraId

Indicates the ID of the camera. This value is fixed in this product.

Requires user role: ADMIN

Value space: `<1>`

Range: Indicates the ID of the camera.

Video Input Source [1..2] OptimalDefinition Profile

The Video Input Source Quality setting must be set to Motion for the optimal definition settings to take any effect.

The optimal definition profile should reflect the lighting conditions in your room and the quality of the video input (camera); the better the lighting conditions and video input, the higher the profile. Then, in good lighting conditions, the video encoder will provide better quality (higher resolution or frame rate) for a given call rate.

Generally, we recommend using the Normal or Medium profiles. However, when the lighting conditions are good, the High profile can be set in order to increase the resolution for a given call rate.

Some typical resolutions used for different optimal definition profiles, call rates and transmit frame rates are shown in the table below. It is assumed that dual video is not used. The resolution must be supported by both the calling and called systems.

Use the Video Input Source OptimalDefinition Threshold60fps setting to decide when to use the 60 fps frame rate.

Typical resolutions used for different optimal definition profiles, call rates and frame rates

Frame rate	Optimal Definition Profile	Call rate						
		256 kbps	*768 kbps*	*1152 kbps*	*1472 kbps*	*2560 kbps*	*4 Mbps*	*6 Mbps*
30 fps	*Normal*	512×288	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080
	Medium	640×360	1280×720	1280×720	1280×720	1920×1080	1920×1080	1920×1080
	High	768×448	1280×720	1280×720	1920×1080	1920×1080	1920×1080	1920×1080
60 fps	*Normal*	256×144	512×288	768×448	1024×576	1280×720	1280×720	1920×1080
	Medium	256×144	768×448	1024×576	1024×576	1280×720	1920×1080	1920×1080
	High	512×288	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080

Requires user role: ADMIN

Value space: `<Normal/Medium/High>`

Normal: Use this profile for a normally to poorly lit environment. Resolutions will be set rather conservative.

Medium: Requires good and stable lighting conditions and a good quality video input. For some call rates this leads to higher resolution.

High: Requires nearly optimal video conferencing lighting conditions and a good quality video input in order to achieve a good overall experience. Rather high resolutions will be used.

Example: `Video Input Source 1 OptimalDefinition Profile: Medium`

Video Input Source [1..2] OptimalDefinition Threshold60fps

For each video input, this setting tells the system the lowest resolution where it should transmit 60fps. So for all resolutions lower than this, the maximum transmitted framerate would be 30fps, while above this resolution 60fps would also be possible, if the available bandwidth is adequate.

Requires user role: ADMIN

Value space: `<512_288/768_448/1024_576/1280_720/Never>`

512_288: Set the threshold to 512x288.
768_448: Set the threshold to 768x448.
1024_576: Set the threshold to 1024x576.
1280_720: Set the threshold to 1280x720.
Never: Do not set a threshold for transmitting 60fps.

Example: `Video Input Source 1 OptimalDefinition Threshold60fps: 1280_720`

Video Input Source [1..2] Quality

When encoding and transmitting video there will be a trade-off between high resolution and high framerate. For some video sources it is more important to transmit high framerate than high resolution and vice versa. The Quality setting specifies whether to give priority to high frame rate or to high resolution for a given source.

Requires user role: ADMIN

Value space: `<Motion/Sharpness>`

Motion: Gives the highest possible framerate. Used when there is a need for higher frame rates, typically when a large number of participants are present or when there is a lot of motion in the picture.

Sharpness: Gives the highest possible resolution. Used when you want the highest quality of detailed images and graphics.

Example: `Video Input Source 1 Quality: Motion`

Video DefaultPresentationSource

Define which video input source shall be used as the default presentation source (when you press the Presentation key on the remote control). The input source is configured to a video input connector.

Requires user role: USER

Value space: `<1/2>`

Range: Select the video source to be used as the presentation source.

Example: `Video DefaultPresentationSource: 2`

Video Input DVI [2] Type

The official DVI standard supports both digital and analog signals. In most cases the default AutoDetect setting can detect whether the signal is analog RGB or digital. However, in some rare cases when DVI-I cables are used (these cables can carry both the analog and digital signals) the auto detection fails. This setting makes it possible to override the AutoDetect and select the correct DVI video input.

Requires user role: ADMIN

Value space: `<AutoDetect/Digital/AnalogRGB/AnalogYPbPr>`

AutoDetect: Set to AutoDetect to automatically detect if the signal is analog RGB or digital.
Digital: Set to Digital to force the DVI video input to Digital when using DVI-I cables with both analog and digital pins and AutoDetect fails.
AnalogRGB: Set to AnalogRGB to force the DVI video input to AnalogRGB when using DVI-I cables with both analog and digital pins and AutoDetect fails.
AnalogYPbPr: Set to AnalogYPbPr to force the DVI video input to AnalogYPbPr, as the component (YPbPr) signal cannot be auto detected.

Example: `Video Input DVI 2 Type: AutoDetect`

Video Layout Scaling

Define how the system shall adjust the aspect ratio for images or frames when there is a difference between the image and the frame it is to be placed in.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Let the system automatically adjust aspect ratio.
Off: No adjustment of the aspect ratio.

Example: `Video Layout Scaling: On`

Video Layout ScaleToFrame

Define what to do if the aspect ratio of a video input source doesn't match the aspect ratio of the corresponding image frame in a composition. For example if you have a 4:3 input source (like XGA) to be displayed on a 16:9 output (like HD720).

Requires user role: ADMIN

Value space: `<Manual/MaintainAspectRatio/StretchToFit>`

Manual: If the difference in aspect ratio between the video input source and the target image frame is less than the ScaleToFrameThreshold configuration (in percent), the image is stretched to fit. If not, the system will maintain the original aspect ratio.
MaintainAspectRatio: Will maintain the aspect ratio of the input source, and fill in black in the rest of the frame (letter boxing or pillar boxing).
StretchToFit: Will stretch (horizontally or vertically) the input source to fit into the image frame. NOTE: The general limitation is that you cannot upscale in one direction and at the same time downscale in the other direction. In such situations the codec will apply letterboxing.

Example: `Video Layout ScaleToFrame: MaintainAspectRatio`

Video Layout ScaleToFrameThreshold

Only applicable if the ScaleToFrame configuration is set to manual. If the difference in aspect ratio between the video input source and the target image frame is less than the ScaleToFrameThreshold configuration (in percent), the image is stretched to fit. If not, the system will maintain the original aspect ratio.

Requires user role: ADMIN

Value space: `<0..100>`

Range: Select a value from 0 to 100 percent.

Example: `Video Layout ScaleToFrameThreshold: 5`

Video SelfviewPosition

Select where the small selfview PiP (Picture-in-Picture) will appear on screen.

Requires user role: ADMIN

Value space: `<UpperLeft/UpperRight/LowerLeft/LowerRight/CenterRight>`

UpperLeft: The selfview PiP will appear in the upper left corner of the screen.
UpperRight: The selfview PiP will appear in the upper right corner of the screen.
LowerLeft: The selfview PiP will appear in the lower left corner of the screen.
LowerRight: The selfview PiP will appear in the lower right corner of the screen.
CenterRight: The selfview PiP will appear in to the right side of the screen, in center.

Example: `Video SelfviewPosition: LowerRight`

Video Layout LocalLayoutFamily

Select which video layout family to be used locally.

Requires user role: ADMIN

Value space: `<Auto/FullScreen/Equal/PresentationSmallSpeaker/PresentationLargeSpeaker>`

Auto: The default layout family, as given in the layout database provided by the system, will be used as the local layout.
FullScreen: The FullScreen layout family will be used as the local layout.
Equal: The Equal layout family will be used as the local layout.
PresentationSmallSpeaker: The PresentationSmallSpeaker layout family will be used as the local layout.
PresentationLargeSpeaker: The PresentationLargeSpeaker layout family will be used as the local layout.

Example: `Video Layout LocalLayoutFamily: Auto`

Video Layout RemoteLayoutFamily

Select which video layout family to be used for the remote participants.

Requires user role: ADMIN

Value space: `<Auto/FullScreen/Equal/PresentationSmallSpeaker/PresentationLargeSpeaker>`

Auto: The default layout family, as given by the local layout database, will be used as the remote layout. For more information about the layout database, see the command: xCommand Video Layout LoadDb.
FullScreen: The FullScreen layout family will be used as the remote layout.
Equal: The Equal layout family will be used as the remote layout.
PresentationSmallSpeaker: The PresentationSmallSpeaker layout family will be used as the remote layout.
PresentationLargeSpeaker: The PresentationLargeSpeaker layout family will be used as the remote layout.

Example: `Video Layout RemoteLayoutFamily: Auto`

Video MainVideoSource

Define which video input source shall be used as the main video source. The video input source is configured with the " Video Input Source [1..2] Connector" setting.

Requires user role: USER

Value space: `<1/2>`

Range: Select the source to be used as the main video source.

Example: `Video MainVideoSource: 1`

Video Monitors

Set the monitor layout mode.

Requires user role: ADMIN

Value space: `<Single/Dual/DualPresentationOnly>`

Single: The same layout is shown on all monitors.
Dual: The layout is distributed on two monitors.
DualPresentationOnly: All participants in the call will be shown on the first monitor, while the presentation (if any) will be shown on the second monitor.

Example: `Video Monitors: Single`

Video OSD Mode

The Video OSD (On Screen Display) Mode lets you define if information and icons should be displayed on screen.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Display the on screen menus, icons and indicators.
Off: Hide the on screen menus, icons and indicators.

Example: `Video OSD Mode: On`

Video OSD AutoSelectPresentationSource

Determine if the presentation source should be automatically selected.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable automatic selection of the presentation source.
Off: Disable automatic selection of the presentation source.

Example: `Video OSD AutoSelectPresentationSource: Off`

Video OSD TodaysBookings

This setting can be used to display the systems bookings for today on the main OSD menu. This requires that the system is bookable by an external booking system, like Cisco TelePresence Management Suite (TMS).

Requires user role: ADMIN

Value space: `<On/Off>`

On: Displays information about this systems bookings on screen.
Off: Do not display todays bookings.

Example: `Video OSD TodaysBookings: Off`

Video OSD MyContactsExpanded

Set how the local contacts will be displayed in the phone book dialog in the OSD (On Screen Display).

Requires user role: ADMIN

Value space: `<On/Off>`

On: The local contacts in the phone book will be shown in the top level of the phonebook dialog.
Off: The local contacts will be placed in a separate folder called MyContacts in the phonebook dialog.

Example: `Video OSD MyContactsExpanded: Off`

Video OSD Output

The Video OSD (On Screen Display) Output lets you define which monitor should display the on screen menus, information and icons. By default the OSD is sent to the monitor connected to the Video OSD Output 1. If you cannot see the OSD on screen, then you must re-configure the OSD Output. You can do this by entering a key sequence on the remote control, from the web interface, or by a command line interface.

Using the remote control: Press the Disconnect key followed by: * # * # 0 x # (where x is output 1 to 2).

Using the web interface: Open a web browser and enter the IP address of the codec. Open the Advanced Configuration menu and navigate to Video OSD Output and select the video output.

Using a command line interface: Open a command line interface and connect to the codec (if in doubt of how to do this, see the API Guide for the codec). Enter the command: xConfiguration Video OSD Output [1..2] (select the OSD Output)

Requires user role: ADMIN

Value space: `<1/2>`

Range: Select 1 for HDMI output, or select 2 for DVI-I output.

Example: `Video OSD Output: 1`

Video OSD InputMethod InputLanguage

The codec can be enabled for Cyrillic input characters in the menus on screen. NOTE: Requires that xConfiguration Video OSD inputMethod Cyrillic is set to On.

Requires user role: ADMIN

Value space: `<Latin/Cyrillic>`

Latin: Latin characters can be entered when using the remote control (default).
Cyrillic: Cyrillic characters can be entered using the remote control. NOTE: Requires a Cisco TelePresence Remote Control with Cyrillic fonts.

Example: `Video OSD InputMethod InputLanguage: Latin`

Video OSD InputMethod Cyrillic

Set the Cyrillic mode for the menu input language in the menus on screen.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Cyrillic mode is available as a menu input language in the menus on screen. This will enable the setting xConfiguration Video OSD InputMethod InputLanguage.
Off: Cyrillic mode is NOT available as a menu input language in the menus on screen.

Example: `Video OSD InputMethod Cyrillic: Off`

Video OSD LoginRequired

Determine if the system should require the user to login before accessing the On Screen Display (OSD). If enabled, the user must enter his username and his PIN. After the user has logged in he can only execute to the configurations changes and commands allowed by his Role.

Requires user role: ADMIN

Value space: `<On/Off>`

On: The user must log in to access the On Screen Display (OSD).
Off: No login to the OSD is required.

Example: `Video OSD LoginRequired: Off`

Video AllowWebSnapshots

Allow or disallow that snapshots captured by the video input main source can be displayed in the web interface Call Control page.

NOTE: This feature is disabled by default, and must be enabled from the On Screen Display (OSD), from a directly connected Touch controller, or when connected directly to the serial port (COM 1 port) on the codec.

Requires user role: ADMIN

Value space: `<On/Off>`

On: If set to on, a web snapshot can be generated and displayed on the web interface.
Off: The generation of web snapshots is not allowed.

Example: `Video AllowWebSnapshots: Off`

Video Output HDMI [1..2] CEC Mode

The HDMI outputs support Consumer Electronics Control (CEC). When set to on (default is off), and the monitor connected to the HDMI output is CEC compatible and CEC is configured, the system will use CEC to set the monitor in standby when the system enters standby. Likewise the system will wake up the monitor when the system wakes up from standby. Please note that the different manufacturers uses different marketing names for CEC: Anynet+ (Samsung); Aquos Link (Sharp); BRAVIA Sync (Sony); HDMI-CEC (Hitachi); Kuro Link (Pioneer); CE-Link and Regza Link (Toshiba); RIHD (Onkyo); SimpLink (LG); HDAVI Control, EZ-Sync, VIERA Link (Panasonic); EasyLink (Philips); and NetCommand for HDMI (Mitsubishi).

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable CEC control.
Off: Disable CEC control.

Example: `Video Output HDMI 1 CEC Mode: Off`

Video Output HDMI [1..2] MonitorRole

The HDMI monitor role describes what video stream will be shown on the monitor connected to the video output HDMI connector. Applicable only if the " Video > Monitors" configuration is set to dual.

Requires user role: ADMIN

Value space: `<First/Second/PresentationOnly>`

First: Show main video stream.
Second: Show presentation video stream if active, or other participants.
PresentationOnly: Show presentation video stream if active, and nothing else.

Example: `Video Output HDMI 1 MonitorRole: First`

Video Output HDMI [1..2] OverscanLevel

Some TVs or other monitors may not display the whole image sent out on the systems video output, but cuts the outer parts of the image. In this case this setting can be used to let the system not use the outer parts of video resolution. Both the video and the OSD menu will be scaled in this case.

Requires user role: ADMIN

Value space: `<Medium/High/None>`

Medium: The system will not use the outer 3% of the output resolution.
High: The system will not use the outer 6% of the output resolution
None: The system will use all of the output resolution.

Example: `Video Output HDMI 1 OverscanLevel: None`

Video Output HDMI [1, 2] Resolution

Select the preferred resolution for the monitor connected to the video output HDMI connector. This will force the resolution on the monitor.

Requires user role: ADMIN

Value space: `<Auto/1024_768_60/1280_1024_60/1280_720_60/1920_1080_60/1280_768_60/1360_768_60/1366_768_60>`

Auto: The system will automatically try to set the optimal resolution based on negotiation with the connected monitor.
Range: 1024x768@60p, 1280x1024@60p, 1280x720@60p, 1920x1080@60p, 1280x768@60p, 1360x768@60p, 1366x768@60p

Example: `Video Output HDMI 1 Resolution: 1920_1080_60`

Video Selfview

Determine if the main video source (selfview) shall be displayed on screen.

Requires user role: USER

Value space: `<On/Off>`

On: Display selfview on screen.
Off: Do not display selfview on screen.

Example: `Video Selfview: On`

Video WallPaper

Select a background image for the video screen when idle. The background image on the Touch controller is not changed.

Requires user role: USER

Value space: `<None/Growing/Summersky/Custom/Wallpaper01/Wallpaper02/Wallpaper03/Wallpaper04/Wallpaper05/Wallpaper06/Wallpaper07/Wallpaper08/Wallpaper09/Wallpaper10/Wallpaper11/Wallpaper12>`

None: There will not be a background image on the screen.
Summersky, Growing, Waves: The selected background image will be shown on the video screen.
Wallpaper01 to Wallpaper12: The selected background image will be shown on both the video screen and the Touch controller.
Custom: If a custom wallpaper is uploaded to the system, it will be used as background image on the screen. If not, there will be no background image.
Use the web interface to upload a custom wallpaper to the video system.
1) On the codec: With a remote control, open the menu on screen and go to Home > Settings > System information to find the IP address. With a Touch controller, tap More > Settings > System Information to find the IP address.
2) On your computer: Open a web browser and enter the IP address of the codec in the address bar. Hover the mouse over the Configuration tab and select " Wallpaper". Browse for the file and press the " Upload" button. The maximum supported resolution is 1920x1200.

Example: `Video Wallpaper: Wallpaper01`

The Experimental settings

The Experimental settings are beta preview features and can be used 'as is'. They are not fully documented.

NOTE: The Experimental settings are likely to change without further notice.

Experimental Audio EcReferenceDelay

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<0..300>`

Example: `Experimental Audio EcReferenceDelay: 0`

Experimental CapsetFilter

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<S: 0, 100>`

Example: `Experimental CapsetFilter: ""`

Experimental CapsetReduction

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<Auto/Reduced>`

Example: `Experimental CapsetReduction: Auto`

Experimental Conference [1..1] PacketLossResilience ForwardErrorCorrection

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Will enable ForwardErrorCorrection (RFC5109) mechanism as part of the PacketLossResilience mechanism. Default value is On.

On: Forward error correction will be used as part of the PacketLossResilience mechanism.

Off: Forward error correction will NOT be used as part of the PacketLossResilience mechanism.

Requires user role: ADMIN

Value space: `<On/Off>`

Example:
```
Experimental Conference 1 PacketLossResilience
ForwardErrorCorrection: On
```

Experimental Conference [1..1] PacketLossResilience RateAdaption

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Will use the a RateAdaption algorithm adapted to the PacketLossResilience mechanism. Default value is On.

Requires user role: ADMIN

Value space: `<On/Off>`

On: RateAdaption will be used as part of the PacketLossResilience mechanism.
Off: RateAdaption will NOT be used as part of the PacketLossResilience mechanism.

Example: `Experimental Conference 1 PacketLossResilience RateAdaption: On`

Experimental Conference [1..1] Multistream Mode

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<Off/On>`

Example: `Experimental Conference 1 Multistream Mode: Off`

Experimental Conference [1..1] Multistream InputCount

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change

Requires user role: ADMIN

Value space: `<1..4>`

Example: `Experimental Conference 1 Multistream InputCount: 1`

Experimental Conference [1..1] Multistream OutputCount

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change

Requires user role: ADMIN

Value space: `<1..4>`

Example: `Experimental Conference 1 Multistream OutputCount: 1`

Experimental Conference [1..1] Multistream Stream [1..4] Source

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<1/2>`

Example: `Experimental Conference 1 Multistream Stream 1 Source: 1`

Experimental Conference [1..1] ReceiverBasedDownspeeding

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<On/Off>`

Example: `Experimental Conference 1 ReceiverBasedDownspeeding: Off`

Experimental CustomSoftbuttons HoldResume

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

This configuration is used to enable Call Hold and Resume in the OSD. Note that Call Hold and Resume will be available even if this setting is set to Off, if Multiway is configured.

Requires user role: ADMIN

Value space: `<Off/On>`

Off: Call Hold and Resume is not available (unless Multiway is configured).

On: Call Hold/Resume is available while the system is in a call. It will be available on softbuttons, and when receiving incoming calls the user will have the option of holding any current calls while accepting the new call.

Example: `Experimental CustomSoftbuttons HoldResume: Off`

Experimental CustomSoftbuttons State [1..2] SoftButton [1..5] Type

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<NotSet/MainSource/PresentationSource/CameraPreset/Actions/SpeedDial>`

Example: `Experimental CustomSoftbuttons State 1 Softbutton 1 Type: NotSet`

Experimental CustomSoftbuttons State [1..2] SoftButton [1..5] Value

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<S: 0, 255>`

Example: `Experimental CustomSoftbuttons State 1 Softbutton 1 Value: ""`

Experimental NetworkServices UPnP Mode

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<On/Off>`

Example: `Experimental NetworkServices UPnP Mode: Off`

Experimental NetworkServices UPnP Timeout

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<0..3600>`

Example: `Experimental NetworkServices UPnP Timeout: 0`

Experimental CTMSSupport Mode

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

This configuration tells whether CTMS (Cisco TelePresence Multipoint Switch) is supported or not.

Requires user role: ADMIN

Value space: `<Off/On>`

Off: CTMS is not supported.

On: CTMS is supported.

Example: `Experimental CTMSSupport Mode: On`

Experimental SystemUnit MenuType

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<Indicators/Full>`

Example: `Experimental SystemUnit MenuType: Full`

Experimental SystemUnit SoftwareUpgrade RequireAuthentication

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<On/Off>`

Example: `Experimental SystemUnit SoftwareUpgrade RequireAuthentication: Off`

Experimental SystemUnit CrashReporting Mode

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<Off/On>`

Example: `Experimental SystemUnit CrashReporting Mode: Off`

Experimental SystemUnit CrashReporting URI

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<S: 0, 255>`

Example: `Experimental SystemUnit CrashReporting URI: ""`

Appendices

Setting the system password

You need a username and password to sign in to the web and command line interfaces of your system.

The video conference system is delivered with a default user account with username admin and no password set. This user has full access rights to the system.

NOTE: We strongly recommend that you set a password for the admin user to restrict access to system configuration.

Make sure to keep a copy of the password in a safe place. You have to contact your Cisco representative if you have forgotten the password.

Changing your system password

Perform the following steps to change the system password.

If a password is currently not set, use a blank *Current password*; to remove a password, leave the *New password* fields blank.

1. Sign in to the web interface with your username and current password.
2. Click your username in the upper right corner and select *Change password* in the drop down menu.
3. Enter the *Current password*, the *New password*, and repeat the new password in the appropriate input fields.

   The password format is a string with 0–64 characters.
4. Click *Change password*.

Changing another user's system password

Read more about creating more user accounts in the ▸ User administration section.

If you have ADMIN rights, you can change all users' passwords by performing the following steps:

1. Sign in to the web interface with your username and password.
2. Go to the *Maintenance* tab and select *User Administration*.
3. Select the appropriate user from the list.
4. Enter a new password and PIN code.
5. Click *Save*.

Setting the Administrator settings menu password

When starting up the system for the first time the Administrator Settings menu password is not set.

NOTE: We strongly recommend that you define a password to protect the Administrator Settings menu, since these settings affect the behavior of the video conference system.

When you set a password for the Administrator settings menu, all users must enter the password to get access to this menu, either on screen when using the remote control, or on the touch screen if you are using a Touch controller.

The menu password can be set from the on-screen menu, using the remote control or from the command line interface; you neither can use a Touch controller nor the web interface.

Setting the Administrator Settings menu password using the remote control

1. In the on screen menu, go to *Home > Settings > Administrator settings > Set menu password*.

   The password format is a string with 0–255 characters.

   To deactivate the password leave the password input field empty.

2. Enter the menu password in the input field. The password you enter is hidden; each character is replaced with a star (*).

   On the remote control, press the # key to toggle between lower or upper case characters and numbers: abc/ABC/123.

3. Select *Save* to save the changes, or *Cancel* to leave without saving.

4. Press *Home* (⌂) to exit.

Setting the Administrator Settings menu password from a command line interface

1. Connect to the system through the network or the serial data port, using a command line interface (SSH or Telnet).

2. Type the following command:

   ```
   xCommand SystemUnit MenuPassword Set
   Password: <password>
   ```

   The password format is a string with 0–255 characters.

Setting a root password

You can protect the file system of your video system by setting a password for the root user. The root user is disabled by default. You have to use the command line interface to enable the root user and set a root password.

Setting a root password

Perform the following steps to activate the root user and set a password for it:

1. Connect to the system through the network or the serial data port, using a command line interface (SSH or Telnet).
2. Sign in to the system with username and password. The user needs ADMIN rights.
3. Type the following command:

```
systemtools rootsettings on <password>
```

NOTE: The root password is not the same as the system (admin) password.

Optimal definition profiles

Under ideal lighting conditions the bandwidth (call rate) requirements can be substantially reduced.

The optimal definition profile should reflect the lighting conditions in your room and the quality of the video input (camera); the better the lighting conditions and video input, the higher the profile. Then, in good lighting conditions, the video encoder will provide better quality (higher resolution or frame rate) for a given call rate.

In general, we recommend the optimal definition profile set to Medium. However, if lighting conditions are very good or bad we recommend that you test the endpoint on the various Optimal Definition Profile settings before deciding on a profile.

Go to Advanced Configuration on the web interface and navigate to *Video > Input > Source [1..n] > OptimalDefinition > Profile* to select the preferred optimal definition profile.

You can set a resolution threshold below which the maximum frame rate will be 30 fps.

Go to Advanced Configuration on the web interface and navigate to *Video > Input > Source [1..n] > OptimalDefinition > Threshold60fps* to set the threshold.

The video input quality settings must be set to Motion for the optimal definition settings to take any effect. With the video input quality set to Sharpness, the endpoint will transmit the highest resolution possible, regardless of frame rate.

Go to Advanced Configuration on the web interface and navigate to *Video > Input > Source [1..n] > Quality* to set the video quality parameter to Motion.

You can read more about these video settings in the
▸ Advanced settings chapter.

High

Typically used in dedicated video conferencing rooms. Requires very good lighting conditions and a good quality video input to achieve a good overall experience.

Under ideal conditions the bandwidth requirements can be reduced by up to 50% compared to Normal.

Medium

Typically used in rooms with good and stable lighting conditions and a good quality video input.

The bandwidth requirements can be reduced by up to 25% compared to Normal.

Normal

This setting is typically used in office environments where the room is normally to poorly lit.

Typical resolutions used for different optimal definition profiles, call rates and frame rates

Frame rate	Optimal Definition Profile	Call rate						
		256 kbps	*768 kbps*	*1152 kbps*	*1472 kbps*	*2560 kbps*	*4 Mbps*	*6 Mbps*
30 fps	*Normal*	512×288	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080
	Medium	640×360	1280×720	1280×720	1280×720	1920×1080	1920×1080	1920×1080
	High	768×448	1280×720	1280×720	1920×1080	1920×1080	1920×1080	1920×1080
60 fps	*Normal*	256×144	512×288	768×448	1024×576	1280×720	1280×720	1920×1080
	Medium	256×144	768×448	1024×576	1024×576	1280×720	1920×1080	1920×1080
	High	512×288	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080

ClearPath – Packet loss resilience

ClearPath introduces advanced packet loss resilience mechanisms that increase the experienced quality when you use your video system in an error prone environment.

To configure ClearPath select *Advanced Configuration* on the web interface and navigate to *Conference 1 > PacketLossResilience > Mode.* Select **Off** to disable ClearPath and select **On** to enable ClearPath.

We recommend that you keep ClearPath enabled on your video system.

Technical specification for SX20 Quick Set

Product compatibility

Fully compatible with standards-compliant telepresence and video systems

Software compatibility

Cisco TelePresence Software Version TC5.1 or later

Components

Set delivered complete with:

- SX20 Codec
- PrecisionHD 1080p 4xS2 or PrecisionHD 1080p 12x camera
- Cisco TelePresence Table Microphone 20
- Remote control
- Cables
- Power supply

Bandwidth

H.323 and SIP up to 6 Mbps point-to-point

Firewall traversal

- Cisco TelePresence Expressway technology
- H.460.18 and H.460.19 firewall traversal

Video standards

- H.263
- H.263+
- H.264

Video features

- Native 16:9 widescreen
- Advanced screen layouts
- Intelligent video management
- Local auto-layout

Video inputs (two inputs)

One HDMI and one DVI-I (analog and digital) input; supported formats:

- 640 × 480
- 720 × 480
- 720 × 576
- 800 × 600
- 848 × 480
- 1024 × 768
- 1152 × 864
- 1280 × 720
- 1280 × 1024
- 1280 × 768
- 1280 × 800
- 1280 × 960
- 1360 × 768
- 1366 × 768
- 1400 × 1050
- 1440 × 900
- 1680 × 1050
- 1920 × 1080

Extended Display Identification Data (EDID)

Video outputs (two outputs)

Two HDMI outputs; supported formats:

- 1920 × 1080@60fps (1080p60)
- 1920 × 1080@50fps (1080p50)
- 1280 × 720@60fps (720p60)
- 1280 × 720@50fps (720p50)
- 1366 × 768@60fps (WXGA)
- 1360 × 768@60fps (WXGA)
- 1280 × 768@60fps (WXGA)

VESA Monitor Power Management

Extended Display Identification Data (EDID)

Live video resolutions (encode/decode):

- 176 × 144@30, 60fps (QCIF) (decode only)
- 352 × 288@30, 60fps (CIF)
- 512 × 288@30, 60fps (w288p)
- 576 × 448@30, 60fps (448p)
- 768 × 448@30, 60fps (w448p)
- 704 × 576@30, 60fps (4CIF)
- 1024 × 576@30, 60fps (w576p)
- 640 × 480@30, 60fps (VGA)
- 800 × 600@30, 60fps (SVGA)
- 1024 × 768@30, 60fps (XGA)
- 1280 × 768@30, 60fps (WXGA)
- 1280 × 720@30, 60fps (HD720p)
- 1920 × 1080@30, 60fps (HD1080p)

Audio standards

- G.711
- G.722
- G.722.1
- 64 kbps MPEG-4 AAC-LD

Audio features

- CD-quality 20 kHz mono
- Two acoustic echo cancellers
- Automatic gain control (AGC)
- Automatic noise reduction
- Active lip synchronization

Audio inputs (four inputs)

- Two microphones, 4-pin minijack
- One minijack for line in (stereo)
- One audio in from camera (HDMI)

Audio outputs (two outputs)

- One minijack for line out (stereo)
- One HDMI (digital main audio)

Dual stream

- H.239 (H.323) dual stream
- BFCP (SIP) dual stream
- Support for resolutions up to 1080p (1920 × 1080)

Multipoint support

- Four-way embedded SIP/H.323 MultiPoint, ref. MultiSite
- Cisco TelePresence Multiway support (requires Cisco TelePresence Video Communication Server [Cisco VCS] and Cisco TelePresence MCU)
- Ability to natively join multipoint conferences hosted on Cisco Telepresence Multipoint Switch (CTMS)

MultiSite features (embedded multipoint switch)

- Four-way SIP/H.323 MultiSite; resolution up to 576p30
- Full individual audio and video transcoding
- Individual layouts in multisite continuous presence (takes out selfview)
- H.323/SIP/VoIP in the same conference
- Support for Presentation (H.239/BFCP) from any participant at resolutions up to 1080p15
- Best Impression (automatic continuous presence layouts)
- H.264, encryption, dual stream from any site
- IP Downspeeding
- Dial in and dial out
- Additional telephone call (no license required)
- Conference rates up to 6 Mbps

Protocols

- H.323
- SIP

Embedded encryption

- H.323 and SIP point-to-point
- Standards-based: H.235 v3 and Advanced Encryption Standard (AES)
- Automatic key generation and exchange
- Support in dual stream

IP network features

- Domain Name System (DNS) lookup for service configuration
- Differentiated services (quality of service (QoS))
- IP adaptive bandwidth management (including flow control)
- Auto gatekeeper discovery
- Dynamic playout and lip-sync buffering
- H.245 dual-tone multifrequency (DTMF) tones in H.323
- Date and time support using the Network Time Protocol (NTP)
- Packet loss based downspeeding
- Uniform resource identifier (URI) dialing
- TCP/IP

- Dynamic Host Configuration Protocol (DHCP)
- IEEE 802.1x network authentication
- IEEE 802.1q VLAN
- IEEE 802.1p QoS and class of service
- ClearPath

IPv6 network support

- Single call stack support for both H.323 and SIP
- Dual-stack IPv4 and IPv6 for DHCP, SSH, HTTP, HTTPS, DNS and DiffServ
- Support for both static and autoconfiguration (stateless address autoconfiguration)

Cisco unified communications manager

(requires Cisco UCM version 8.6 or later)

- Native registration with Cisco Unified Communications Manager
- Basic Cisco Unified Communications Manager provisioning
- Firmware upgrade from Cisco Unified Communications Manager
- Cisco Discovery Protocol and DHCP option 150 support
- Basic telephony features such as hold, resume, transfer, and corporate directory lookup

Security features

- Management using HTTPS and SSH
- IP administration password
- Menu administration password
- Disable IP services
- Network settings protection

Network interfaces

- One LAN and Ethernet (RJ-45) 10/100/1000 Mbps

Other interfaces

- Two USB host for future use

PrecisionHD 1080p 12x camera

- 1/3” CMOS
- 12 × zoom
- +15°/-25° tilt
- +/- 90° pan
- 43.5° vertical field of view
- 72° horizontal field of view
- Focus distance 0.3 m – infinity
- 1920 × 1080 pixels progressive at 60 fps
- Other formats supported (configurable through Dip-switch): 1920 × 1080@60 fps (HDMI only), 1920 × 1080@50 fps (HDMI only), 1920 × 1080@30 fps, 1920 × 1080@25 fps, 1280 × 720@60 fps, 1280 × 720@50 fps, 1280 × 720@30 fps, 1280 × 720@25 fps
- Automatic or manual focus / brightness / white balance
- Far-end camera control
- Dual HDMI and HD-SDI output
- Upside-down mounting with automatic flipping of picture

PrecisionHD camera 1080p 4xS2

- 1/3” CMOS
- 4 × zoom
- +15°/-25° tilt
- +/- 90° pan
- 43.5° vertical field of view
- 70° horizontal field of view
- Focus distance 0.3 m – infinity
- 1920 × 1080 pixels progressive at 60 fps
- Automatic or manual focus / brightness / white balance
- Far-end camera control
- Upside-down mounting with manual flipping of picture

System management

- Support for the Cisco TelePresence Management Suite
- Total management using embedded SNMP, Telnet, SSH, XML and SOAP
- Remote software upload using web server, SCP, HTTP and HTTPS

Directory services

- Support for local directories (My Contacts)
- Corporate directory
- Unlimited entries using server directory supporting Lightweight Directory Access Protocol (LDAP) and H.350 (available with Cisco TelePresence Management Suite)
- Unlimited number for corporate directory (available with Cisco TelePresence Management Suite)
- Received calls with date and time
- Placed calls with date and time
- Missed calls with date and time

User interface

- Remote control and on-screen menu
- Cisco TelePresence Touch (optional)

Power

- Autosensing power supply
- 100 – 240 VAC, 50/60 Hz
- Maximum 40 watts for codec and main camera

Temperature range

Operating temperature and humidity:

- Ambient temperature: 32° F to 95° F (0° C to 35° C)
- Relative humidity (RH): 10% to 90%

Storage and transport temperature:

- –4° F to 140° F (–20° C to 60° C) at RH 10% to 90% (non-condensing)

SX20 Codec dimensions

- Width: 300 mm / 11.8 in.
- Height: 34 mm / 1.4 in.
- Depth: 180 mm / 7.1 in.
- Weight: 1.4 kg / 3.1 lb

Approvals and compliance

EU/EEC

Directive 2006/95/EC (Low Voltage Directive)

- Standard IEC/EN 60950-1

Directive 2004/108/EC (EMC Directive)

- Standard EN 55022, Class A
- Standard EN 55024
- Standard EN 61000-3-2/-3-3

Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

USA

Approved according to UL 60950-1.

Complies with FCC CFR 15B Class A.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canada

Approved according to CAN/CSA C22.2 No. 60950-1-07.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

All specifications are subject to change without notice, system specifics may vary.

All images in these materials are for representational purposes only, actual products may differ.

February 2012

Supported RFCs

The RFC (Request for Comments) series contains technical and organizational documents about the Internet, including the technical specifications and policy documents produced by the Internet Engineering Task Force (IETF).

The information on this page appilies to Cisco TelePresence video systems running TC software:

- Cisco TelePresence Codec C Series (C90, C60, C40)
- Cisco TelePresence Profile Series using Codec C Series
- Cisco TelePresence EX Series (EX90, EX60)
- Cisco TelePresence MX Series (MX300, MX200)
- Cisco TelePresence Quick Set Series (C20, SX20)

Current RFCs and drafts supported

- RFC 1889 RTP: A Transport Protocol for Real-time Applications
- RFC 2190 RTP Payload Format for H.263 Video Streams
- RFC 2396 Uniform Resource Identifiers (URI): Generic Syntax
- RFC 2429 RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)
- RFC 2460 Internet protocol, version 6 (IPv6) specification
- RFC 2617 Digest Authentication
- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 2976 The SIP INFO Method
- RFC 3016 RTP Payload Format for MPEG-4 Audio/Visual Streams
- RFC 3047 RTP Payload Format for ITU-T Recommendation G.722.1
- RFC 3261 SIP: Session Initiation Protocol
- RFC 3262 Reliability of Provisional Responses in SIP
- RFC 3263 Locating SIP Servers
- RFC 3264 An Offer/Answer Model with SDP
- RFC 3311 UPDATE method
- RFC 3361 DHCP Option for SIP Servers
- RFC 3420 Internet Media Type message/sipfrag
- RFC 3515 Refer method
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3581 Symmetric Response Routing
- RFC 3605 RTCP attribute in SDP
- RFC 3711 The Secure Real-time Transport Protocol (SRTP)
- RFC 3840 Indicating User Agent Capabilities in SIP
- RFC 3890 A Transport Independent Bandwidth Modifier for SDP
- RFC 3891 The SIP “Replaces” Header
- RFC 3892 Referred-By Mechanism
- RFC 3960 Early Media
- RFC 4028 Session Timers in SIP
- RFC 4145 TCP-Based Media Transport in the SDP
- RFC 4566 SDP: Session Description Protocol
- RFC 4568 SDP:Security Descriptions for Media Streams
- RFC 4574 The Session Description Protocol (SDP) Label Attribute
- RFC 4582 The Binary Floor Control Protocol
- RFC 4583 SDP Format for BFCP Streams
- RFC 4585 Extended RTP Profile for RTCP-Based Feedback
- RFC 4587 RTP Payload Format for H.261 Video Streams
- RFC 4629 RTP Payload Format for ITU-T Rec. H.263 Video
- RFC 4733 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 4796 The SDP Content Attribute
- RFC 4862 IPv6 stateless address autoconfiguration
- RFC 5168 XML Schema for Media Control
- RFC 5589: SIP Call Control Transfer
- RFC 5626 Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
- RFC 6184 RTP Payload Format for H.264 Video
- RFC 6185 RTP Payload Format for H.264 Reduced-Complexity Decoding Operation (RCDO) *

Media capabilities supported in SIP

The audio and video media capabilities supported in SIP are the same as for H.323.

* Applies to Cisco TelePresece SX20 Quick Set only.

User documentation on the Cisco web site

User documentation for Cisco TelePresence products can be found on ‣ http://www.cisco.com/go/telepresence/docs.

Depending on which product you have got, select the following in the right pane:

MX Series:

TelePresence Endpoints - Multipurpose
> Cisco TelePresence MX Series

Profile Series:

TelePresence Endpoints - Multipurpose
> Cisco TelePresence System Profile Series

EX Series:

TelePresence Endpoints - Personal
> TelePresence Desktop
> Cisco TelePresence System EX Series

Codec C Series:

TelePresence Solutions Platform
> TelePresence Integrator Products
> Cisco TelePresence System Integrator C Series

SX20 Quick Set and Quick Set C20:

TelePresence Solutions Platform
> TelePresence Quick Set
> Cisco TelePresence Quick Set Series

Document categories

For each product you will find the documents under the following categories:

User guides:

Maintain and Operate | End-User Guides

Quick reference guides:

Maintain and Operate | End-User Guides

Installation guides:

Install and Upgrade | Install and Upgrade Guides

Getting started guide:

Install and Upgrade | Install and Upgrade Guides

Administrator guides:

Maintain and Operate | Maintain and Operate Guides

API reference guides:

Reference Guides | Command references

Physical interface guides:

Maintain and Operate | End-User Guides

Regulatory compliance and safety information:

Install and Upgrade | Install and Upgrade Guides

TC software release notes:

Release and General Information | Release Notes

TC software licensing information:

Release and General Information | Licensing Information

Video conferencing room guidelines:

Design | Design Guides

NOTE: All products do not have all types of user documentation.

Intellectual property rights

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

TANDBERG is now a part of Cisco. TANDBERG® is a registered trademark belonging to Tandberg ASA.

Cisco contacts

On our web site you will find an overview of the worldwide Cisco contacts.

Go to: ▸ http://www.cisco.com/web/siteassets/contacts

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA